

1 IN THE DISTRICT COURT OF THE UNITED STATES
2 FOR THE NORTHERN DISTRICT OF OHIO
3 EASTERN DIVISION

4 UNITED STATES OF AMERICA,)
5)
6) Judge Gaughan
7) Cleveland, Ohio
8) Number 1:16CR224
9 BOGDAN NICOLESCU,)
10 RADU MICLAUS,)
11)
12) Defendants.
13)

14 - - - - -
15 TRANSCRIPT OF PROCEEDINGS HAD BEFORE
16 THE HONORABLE PATRICIA ANNE GAUGHAN
17 JUDGE OF SAID COURT,
18 ON TUESDAY, MARCH 26, 2019

19 **Volume 2**
20 - - - - -

21 Official Court Reporter: Shirle M. Perkins, RDR, CRR
22 U.S. District Court
23 801 West Superior, #7-189
24 Cleveland, OH 44113-1829
25 (216) 357-7106

26 Proceedings recorded by mechanical stenography; transcript
27 produced by computer-aided transcription.

1 APPEARANCES:

2 For the Government:

DUNCAN T. BROWN,
BRIAN MCDONOUGH,
Assistant U.S. Attorneys
801 West Superior Avenue
Cleveland, OH 44113
(216) 622-3600

5 BRIAN L. LEVINE,
6 U.S. Department of Justice -
7 Criminal Division
8 Ste. 600
1301 New York Avenue
Washington, DC 20530
(202) 616-5227

9 For Bogdan Nicolescu:

10 MICHAEL GOLDBERG, ESQ.,
Goldberg & O'Shea
Suite 450
11 323 Lake Place
Cleveland, OH 44113
12 (216) 696-4514

13 For Radu Miclaus:

MICHAEL J. O'SHEA, ESQ.,
Lipson O'Shea
14 110 Hoyt Block Bldg.
700 West St. Clair Avenue
15 Cleveland, OH 44113
16 (216) 241-0011

17
18
19
20
21
22
23
24
25

1 TUESDAY SESSION, MARCH 26, 2019, AT 8:43 A.M.

2 (Proceedings in the absence of the jury:)

3 THE COURT: I have been informed -- I'm sorry,
4 folks. You can be seated.

09:10:32 5 I have been informed that Juror Number 3 is here but
6 very sick. My Courtroom Deputy is going to have a
7 conversation with her and see if she can stick it out
8 because Ms. Higley, who was Alternate Number 3, had a
9 medical emergency and is not here. And she is Alternate
09:11:21 10 Number 3.

11 MR. BROWN: Your Honor, not to be morbid, I
12 guess, but is the medical emergency just a one-day thing
13 or --

14 THE COURT: Mr. Brown, I -- I don't have a
09:11:35 15 clue. I don't even know if it's made up. I know nothing.

16 MR. BROWN: Okay. So we have two alternates,
17 and if we are going to excuse Ms. Zanath, we are down to one
18 alternate. And off the record.

19 (Proceedings held off the record.)

09:12:56 20 THE COURT: Ms. Zanath has indicated to my
21 Courtroom Deputy that she doesn't believe she can make it
22 today. Is that correct, Stella?

23 DEPUTY CLERK: Yes.

24 MR. O'SHEA: That's Number 3, Judge?

09:13:07 25 THE COURT: That's Number 3. She was 13, and

1 then she became Number 3.

2 MR. GOLDBERG: Judge, I don't know how we do
3 it. I don't see how we go forward with one alternate. So
4 I -- in the interest of this being the trial and having to
09:13:37 5 start over, I would say that we recess for the day, as much
6 as I hate to say it, but to go with one alternate for this
7 case -- that's why we asked for four.

8 MR. O'SHEA: And at the expense of agreeing
9 with Mr. Goldberg, I agree with Mr. Goldberg.

09:14:02 10 MR. BROWN: That would be the idea, that one
11 day might give Juror Number 3 the opportunity to --

12 MR. O'SHEA: Recover.

13 MR. BROWN: -- drink fluids, get better and
14 recover.

09:14:12 15 MR. GOLDBERG: And the alternate.

16 MR. BROWN: And the alternate, I guess. And
17 also the -- save all future illnesses.

18 MR. O'SHEA: Good point. Probably infecting
19 each other.

09:22:21 20 THE COURT: Ms. Zanath has indicated that she
21 will stay and we can proceed. And if she has a coughing
22 fit, she indicated to Stella she doesn't know what to do.
23 And so I'm assuring her through Stella that she has -- she
24 can bring water in or any beverage in the courtroom plus
09:22:45 25 cough drops, and if that occurs, we will simply pause,

1 wherever you are in the questioning.

2 Regarding Ms. Higley, she had e-mailed at 5:00 A.M.
3 this morning indicating that she had to go to the hospital.
4 We do not know if it's her own personal issue or a family
09:23:08 5 issue.

6 Natalie from the jury room has been trying to reach
7 her to get more information. And she hasn't been able to
8 contact her. She did leave a voice mail. I'm going to give
9 it about another ten minutes, and if we don't hear back from
09:23:28 10 her, I think we'll just proceed and replace her.

11 Is that acceptable to the Government?

12 MR. BROWN: Yes, your Honor.

13 THE COURT: Mr. Goldberg?

14 MR. GOLDBERG: It's acceptable, your Honor.

09:23:41 15 I'm concerned about proceeding with one alternate, but
16 that -- that's acceptable.

17 THE COURT: No, we would have -- no, two
18 alternates.

19 MR. GOLDBERG: We have two alternates and we
09:23:53 20 have one juror that we thought was maybe not going to be
21 here and we excused. She will be here?

22 THE COURT: She will be here.

23 MR. GOLDBERG: Okay.

24 THE COURT: So, therefore, we are left with
09:24:02 25 two alternates.

1 MR. GOLDBERG: We're -- yeah, we're fine with
2 that.

3 THE COURT: Mr. O'Shea?

4 MR. O'SHEA: Okay. So Juror Number 3 is here
09:24:08 5 but just not feeling well?

6 THE COURT: Correct.

7 MR. O'SHEA: Okay.

8 THE COURT: Correct. Not feeling well, and
9 she has coughing jags. Stella had another conversation with
09:24:17 10 her and indicated that the Judge is willing to recess for
11 the day as opposed to excusing her. And then she said okay,
12 she'll stay.

13 MR. GOLDBERG: Okay. I guess that's two
14 alternates.

09:24:32 15 THE COURT: Yes.

16 MR. O'SHEA: You guys think it's still two and
17 a half weeks, United States of America?

18 MR. BROWN: Yeah, right. I think -- yes.

19 MR. O'SHEA: There's just a rest. That's all.
09:24:44 20 I mean --

21 THE COURT: Again, you know, I'm going to give
22 it about ten more minutes to see if we get any more
23 information regarding Ms. Higley.

24 MR. O'SHEA: Okay. I guess -- I'll do it.

09:25:01 25 THE COURT: Okay, folks. We're in recess for

1 about another ten minutes.

2 MR. BROWN: Thank you, your Honor.

3 MR. McDONOUGH: Thank you, your Honor.

4 (Thereupon, a recess was taken.)

09:26:12 5 THE COURT: All right. It's 9:35. I think
6 I've given more than ten minutes.

7 DEPUTY CLERK: Okay. We're on the bench.

8 THE COURT: No answer? All right.

9 Folks, Stella tried to call, Natalie's called a couple
09:38:08 10 of times, and we're just not getting any response.

11 So at this point, I believe Ms. Higley is going to be
12 excused for cause.

13 Stella, would you get the jurors.

14 (Proceedings resumed within the presence of the jury:)

09:40:55 15 THE COURT: Ms. Zanath, we know you are not
16 feeling well, but we desperately need all of our jurors.
17 We've already lost a juror. If you do go into a coughing
18 fit, I instructed the attorneys to simply stop the
19 questioning, and if you need a break at any time, just raise
09:41:15 20 your right hand.

21 A JUROR: Okay.

22 THE COURT: Okay. And thank you for being
23 such a trooper.

24 A JUROR: Yeah.

09:41:20 25 THE COURT: Mr. Levine, you may continue

Diaz - Direct/Levine

1 direct examination.

2 MR. LEVINE: Thank you, your Honor.

3 DIRECT EXAMINATION OF STACY DIAZ (cont.)

4 BY MR. LEVINE:

09:41:25 5 Q. Good morning. All right.

6 So when we left off, I was asking you about
7 Government's Exhibit 1324, and if we could please publish
8 1324. I would ask if we could please zoom in on the bottom
9 of the first page on the top half. Okay.

09:42:06 10 So now, at a general level first what is Government's
11 Exhibit 1324?

12 A. This is an e-mail that was provided to me from Read
13 Notify.

14 Q. Okay.

09:42:19 15 And at a general level, who is this e-mail between?

16 A. It is between a member of the Bayrob Group and a
17 potential eBay fraud victim.

18 Q. Okay.

19 And can you explain the context for the e-mail that
09:42:36 20 appears on your screen? What is the context because we're
21 not going to go through the whole chain?

22 A. Correct.

23 So the eBay fraud victim had been communicating with a
24 Bayrob Group member. The potential eBay fraud victim
09:42:51 25 figured out this was a scam.

Diaz - Direct/Levine

1 MR. O'SHEA: Objection.

2 THE COURT: Sustained.

3 MR. LEVINE: So, your Honor, I believe the
4 witness is just providing --

09:43:03 5 THE COURT: Sustained.

6 MR. LEVINE: Okay. So --

7 THE COURT: And, ma'am, would you hold the
8 microphone a little bit closer to you.

9 THE WITNESS: Yes, ma'am.

09:43:13 10 THE COURT: Thank you.

11 BY MR. LEVINE:

12 **Q.** What is the Bayrob Group member responding to in this
13 e-mail?

14 **A.** He is responding to an e-mail from the potential eBay
09:43:25 15 fraud victim.

16 **Q.** Okay. And what -- what had that eBay fraud victim
17 proposed?

18 MR. GOLDBERG: Objection.

19 THE COURT: Proposed?

09:43:34 20 MR. LEVINE: Yes. Your Honor, the -- as we
21 discussed --

22 THE COURT: You know, not in front of the
23 jury.

24 MR. LEVINE: Okay. Can I --

09:43:41 25 THE COURT: Why don't you rephrase your

Diaz - Direct/Levine

1 question?

2 MR. LEVINE: Okay.

3 Q. All right.

09:43:50

4 What is the Bayrob Group member responding to in this
5 e-mail here that we see?

6 A. It was an e-mail to the Bayrob Group member proposing
7 to work with --

8 MR. GOLDBERG: Objection.

9 THE COURT: Side bar, folks.

09:44:02

10 MR. GOLDBERG: Thank you.

11 (The following proceedings were held at side bar:)

12 THE COURT: My concern is if you're not
13 offering the statements from the victim for the truth of the
14 matter asserted, then what -- why are you -- what is the
15 importance of the statements?

09:44:33

16 She can get out what the context is and what the
17 Bayrob member said without her talking about well, the
18 victim figured out that he or she was a fraud, subject of
19 the fraud.

09:44:51

20 MR. LEVINE: Yes. All I am trying to get
21 her -- so all I'm trying to get her to say is that -- the
22 context for this response, and the -- the context is that
23 the potential victim realizes it's a scam and says -- and
24 tells the Bayrob Group member, and this is the Bayrob Group
09:45:09 25 member's response, and it's very clear as --

Diaz - Direct/Levine

1 THE COURT: What is the Bayrob member's
2 response?

3 MR. LEVINE: That's what's on the screen.

4 THE COURT: Tell me what it is.

09:45:19 5 MR. LEVINE: Bayrob Group member's response
6 is -- has to do with you can assist, maybe you can assist us
7 by calling people on the phone and being someone with an
8 American accent. And he also talks about that we're a group
9 of five people and he gives details.

09:45:36 10 THE COURT: So why not just get that out?

11 MR. LEVINE: That's what I'll do next, but I
12 would just like -- one line of context for the jury so they
13 understand what -- where this is coming from.

14 MR. O'SHEA: And my concern, Judge, and the
09:45:50 15 basis at least of my objections, and I'll let Mr. Goldberg
16 speak for himself, is that is this person going to testify?

17 MR. LEVINE: No, of course not.

18 MR. O'SHEA: Okay. That was just a yes or no
19 question. All right.

20 THE COURT: Hang on.

21 MR. LEVINE: You asked me a question. As we
22 discussed yesterday --

23 THE COURT: No, no, no. The answer is no.
24 The victim's not testifying. Go ahead.

09:46:11 25 MR. O'SHEA: All right.

Diaz - Direct/Levine

1 And in that regard, clearly what the victim is saying
2 here is clearly hearsay. The declarant will be unavailable
3 fits no exception I'm aware of because it's not in
4 furtherance of the conspiracy. So the coconspirator
09:46:26 5 exception doesn't apply.

6 And what the agent's doing in addition to that is
7 saying well, this is what they mean by the words that we
8 see, and that's where a big problem --

9 THE COURT: That was my -- that was my --

09:46:41 10 MR. GOLDBERG: I'm sorry, Judge. That was my
11 objection as well.

12 THE COURT: And that was my concern.

13 MR. BROWN: Your Honor, we could phrase the
14 question to in a response to a conversation, what was the
09:46:49 15 Bayrob Group member's response.

16 THE COURT: Correct.

17 MR. BROWN: Because that helps establish the
18 conspiracy by the statement.

19 THE COURT: I'm fine with that.

09:46:55 20 MR. BROWN: Okay.

21 MR. LEVINE: Okay. That's fine.

22 (Proceedings resumed within the hearing of the jury:)

23 BY MR. LEVINE:

24 Q. Okay. Thank you, your Honor.

09:47:14 25 Okay. So looking at the top of Page 1 and the bottom

Diaz - Direct/Levine

1 of Page 2, and I have a hard copy here if that helps to read
2 it. Just let me know.

3 What -- can you summarize what the Bayrob Group's
4 ultimate response to this e-mail from a victim was?

09:47:36

5 **A.** Yes.

09:47:53

6 The Bayrob Group member responded that it was an
7 interesting idea to have someone in the United States that
8 would be able to talk to potential eBay fraud victims
9 without an accent, someone that would be able to communicate
10 and maybe not throw up a red flag. And that although many
11 people will ask questions, he doesn't like to provide them
12 with a lot of information because then that will just lead
13 to more and more questions.

09:48:17

14 He continues to go on to say that if they were to work
15 out a deal together, so that this person was working with
16 the Bayrob Group, they would provide him with a percentage
17 of the money that is made from their scams. And he says at
18 the bottom that it's approximately five people working
19 together to do these jobs, as he called them, and then asked
20 to have this person talk to him off of e-mail on Instant
21 Messenger instead to further discuss this proposal.

09:48:37

22 **Q.** Okay. Thank you, Agent Diaz.

23 All right. Now can we now look -- and when I say
24 look, I mean just us, not the jury -- at what is
09:49:00 25 Government's Exhibit 1325S.

Diaz - Direct/Levine

1 MR. LEVINE: And, your Honor, just to be
2 clear, I move to admit Government's Exhibit 1324, subject to
3 future confirmation of the conspiracy.

4 THE COURT: You know, why don't we do that
09:49:14 5 later after the other witnesses testify?

6 MR. LEVINE: Okay.

7 BY MR. LEVINE:

8 Q. Special Agent Diaz, what is Exhibit 1325?

9 A. This is another e-mail provided to me from Read
09:49:36 10 Notify.

11 Q. Okay. And is Government's Exhibit 1325 a fair and
12 accurate copy of a Read Notify e-mail as it was produced to
13 you by Read Notify?

14 A. Yes, it is.

09:49:46 15 Q. Okay.

16 And subject to the items that we discussed at the end
17 of the day yesterday, your Honor, and this morning, I'd like
18 to publish, permission to publish 1325 to the jury?

19 THE COURT: You may.

09:50:08 20 MR. LEVINE: Okay.

21 And let me just zoom in on bottom of this e-mail and
22 onto the top of it. Yeah, perhaps right there. Okay.
23 Okay.

24 Q. And on a general level, Special Agent Diaz, who is
09:50:34 25 this e-mail between?

Diaz - Direct/Levine

1 **A.** I don't see it on my screen anymore.

2 THE COURT: Do you see it now?

3 THE WITNESS: Yes.

4 MR. LEVINE: And I'll ask permission to

09:50:49 5 approach the witness for --

6 THE COURT: You don't have to ask. Just

7 approach.

8 MR. LEVINE: Thank you, your Honor. Here's a

9 hard copy.

09:50:58 10 THE WITNESS: Thank you.

11 BY MR. LEVINE:

12 **Q.** I want to step back for one moment. Based on your --

13 looking at the last e-mail that we had, based on your

14 ultimate investigation, is it accurate that there were

09:51:17 15 approximately five core members of the Bayrob Group during

16 certain periods?

17 MR. O'SHEA: Objection.

18 THE COURT: Overruled.

19 THE WITNESS: Yes, that is correct.

09:51:26 20 **Q.** Okay.

21 So looking at Government's Exhibit 1325, you said this

22 is an e-mail between a potential victim and Bayrob Group

23 member?

24 **A.** Yes, I had not said that yet, but yes, that's what it

09:51:47 25 is.

Diaz - Direct/Levine

1 Q. Okay. Thank you.

2 Can you summarize the Bayrob Group's response in this
3 e-mail that is now on the screen?

4 MR. O'SHEA: Objection.

09:51:58 5 THE COURT: Overruled.

6 THE WITNESS: The Bayrob Group member responds
7 that there are basically three types of Americans. There
8 are the ones that fall for his scheme that are stupid and
9 basically if they don't fall for his fraud, they were going
09:52:18 10 to fall for some other fraud eventually because they're that
11 stupid.

12 There are the people that don't fall for his scams,
13 and those are the normal people, and he never has any
14 communication with them.

09:52:29 15 And then there's the vigilantes, and he doesn't
16 understand the vigilantes because they spend so much time on
17 something they don't get anything out of it. So they must
18 be doing it basically to feel better about themselves.
19 They're want to be cops. But then he goes on to continue to
09:52:44 20 discuss cops and how cops are basically bad guys that
21 couldn't make it. So they become police officers to feel
22 better about themselves.

23 And that the fact that the police will never defeat
24 them, will never defeat me, he says. At least they can --
09:53:07 25 at least they feel good when the vigilantes worship them,

Diaz - Direct/Levine

1 and that's so, that's so fucking low he says, and he laughs.

2 But then he gets -- he continues and ends it with, "Do
3 you even have how much money I am making? Why don't you get
4 a life? Ever had one? I find it seriously doubtful."

09:53:31 5 Q. Okay. Thank you, Agent Lough.

6 And the e-mail, the last Paragraph, last large
7 paragraph that begins Number 3, there's a line where the
8 other member says, "I just laugh at them because they can't
9 shut me down before I scam everyone that is scamful."

09:53:57 10 Was it your experience that the scam continued on for
11 many years after this particular e-mail?

12 MR. O'SHEA: Objection.

13 THE COURT: Sustained.

14 Q. Did your investigation show -- what's the date of this
09:54:14 15 particular e-mail?

16 A. July 1, 2010.

17 Q. Okay.

18 And was it your -- did your investigation show that
19 the scam continued for many years after July 1, 2010?

09:54:24 20 MR. O'SHEA: Objection.

21 MR. GOLDBERG: Objection.

22 THE COURT: Sustained to the form of the
23 question.

24 Q. Did you continue to identify victims -- until what
09:54:35 25 point did you continue to identify victims?

Diaz - Direct/Levine

1 **A.** We continued to identify Bayrob e-mail fraud victims
2 until approximately 2013.

3 **Q.** Okay. Thank you, Special Agent Diaz. All right.

4 Now I want to talk about your early efforts to
09:54:57 5 identify the Bayrob Group.

6 Was one of the things the FBI did to investigate the
7 victim -- was one of the things the FBI did to investigate
8 the victim complaints and to analyze the virus on the
9 victims' computers?

09:55:12 10 **A.** Yes, that is correct.

11 **Q.** And in general, what did the FBI's analysis of the
12 virus on Yvonne Liddy's computer and the other victim's
13 computers reveal?

14 **A.** In the very beginning, the virus was primarily there
09:55:27 15 just to help facilitate the eBay fraud. It would redirect
16 the computer so that they had complete control when the
17 victim went to eBay, it could display the content they
18 wanted displayed and not real content from eBay.com. It
19 could do that with other websites, such as Carfax. It would
09:55:49 20 block actually IC3, which we talked about yesterday, which
21 is a website for victims to report the fact that they have
22 been victimized. So their computer would not let them
23 actually visit IC3 because they were infected with the
24 Bayrob trojan.

09:56:05 25 It would also display other fake information showing

Diaz - Direct/Levine

1 them that once they believe they had purchased a vehicle,
2 there was websites that they were directed to, to see that
3 the car was being shipped to them. And so the computer,
4 because it was infected with the Bayrob trojan, would
09:56:20 5 display fake content to them showing them that the car was
6 actually being shipped to their location.

7 **Q.** And was that one way that you knew that this
8 particular victim, whose computer you were examining, was a
9 victim of the Bayrob Group, that they had this virus?

09:56:36 10 **A.** Yes, absolutely.

11 **Q.** Now, did the FBI's analysis of the virus on victims'
12 computers provide information to help specifically identify
13 the Bayrob Group?

14 **A.** Yes -- I'm sorry. I didn't understand the question.

09:56:51 15 **Q.** Okay. Thank you. Did the -- let me try to rephrase
16 it.

17 When the FBI analyzed the virus on the victim's
18 computers, did that provide any information to help
19 specifically identify who the members, the identity of the
09:57:07 20 members of the Bayrob Group?

21 **A.** No, not the actual members of the Bayrob Group.

22 **Q.** Why not?

23 **A.** There were multiple reasons why. We had determined
24 that they were using the infected computers to hide their IP
09:57:21 25 address. They were also taking other steps to hide who they

Diaz - Direct/Levine

1 actually were behind fake e-mail accounts and behind their
2 web -- their virus itself.

3 Q. Okay.

4 So let's just confine it to the virus. Was there
09:57:38 5 anything in the virus that you examined that would help
6 identify either any member of the Bayrob Group?

7 A. No, there was nothing in the virus itself.

8 Q. Okay.

9 Did you also investigate the e-mails between the
09:57:50 10 victims and members of the Bayrob Group?

11 A. Yes.

12 Q. And what did you do to investigate the e-mails that
13 victims had with members of the Bayrob Group?

14 A. So we would review the e-mails themselves, determine
09:58:02 15 what e-mail account they were receiving e-mails from. I
16 would send a subpoena or search warrant to the provider,
17 Yahoo, AOL, whatever company it was, to be able to
18 investigate the entire e-mail account itself.

19 Q. Okay.

09:58:17 20 And in response to your search warrants or your
21 other -- your subpoenas, did you receive records from the
22 e-mail providers?

23 A. Yes.

24 Q. And when you obtained e-mail records from the
09:58:29 25 providers, did the providers also provide information about

Diaz - Direct/Levine

1 the subscribers for those e-mail accounts, such as their
2 name, phone number, address, that sort of thing?

3 **A.** Yes, they did.

4 **Q.** And as a general matter, did that subscriber
09:58:42 5 information you received from the e-mail providers, did that
6 help you identify any of the Bayrob Group members?

7 **A.** No, it did not.

8 **Q.** Why not?

9 **A.** Because they would use fake information, such as John
09:58:53 10 Doe or something along those lines.

11 MR. GOLDBERG: Objection, Judge.

12 THE COURT: Overruled.

13 **Q.** Okay.

14 And when you obtained e-mail records from these
09:59:02 15 providers, did the providers also provide you with IP
16 address information?

17 **A.** Yes, they did.

18 **Q.** What is an IP address?

19 **A.** An IP address is a way to identify the Internet
09:59:13 20 connection that a computer is using. You can think of it
21 similar to like a telephone number.

22 **Q.** Okay.

23 So I'd like to show just for you, and us here,
24 Government's Exhibit 2036, which is a demonstrative for
09:59:33 25 identification.

Diaz - Direct/Levine

1 MR. O'SHEA: Judge.

2 THE COURT: I'm sorry?

3 MR. O'SHEA: We're just trying to pull it up.

4 Okay. No objections.

09:59:44 5 BY MR. LEVINE:

6 Q. Okay. Do you see it there?

7 A. Yes, I do.

8 Q. Thank you.

9 Would Government's Exhibit 2036 help you explain to
09:59:51 10 the jury how you would use an IP address in a typical
11 investigation to help identify a criminal?

12 A. Yes.

13 MR. LEVINE: Your Honor, for purposes -- for
14 demonstrative purposes, the Government would like to publish
10:00:04 15 Government's Exhibit 2036 to the jury.

16 MR. O'SHEA: No objections, Judge.

17 MR. GOLDBERG: No objection.

18 MR. LEVINE: Your Honor, any -- is that okay?

19 THE COURT: It's already on.

10:00:25 20 MR. LEVINE: Oh, it's on. I'm sorry. I
21 thought you were going to rule. Sorry. Dramatic pause.

22 Q. All right. So it's on.

23 So, Special Agent Diaz, if you could use Exhibit 2036
24 to help explain to the jury how you -- how would you use an
10:00:41 25 IP address to help identify a criminal?

Diaz - Direct/Levine

1 **A.** Absolutely.

10:00:56

2 So the Internet Service Provider that you see on the
3 left corner would be like your -- whoever you paid to have
4 Internet at your house. I use WOW Internet. So WOW
5 Internet is my Internet Service Provider. So they assign to
6 me at my house an IP address that is used usually
7 temporarily for Internet connection from a particular
8 location.

10:01:15

9 So my house, I have been assigned 1234 as my IP
10 address from WOW Internet. If I send an e-mail or if I
11 connect to Gmail, to send e-mail, Gmail is going to see me
12 coming from IP address 1234. That's all that they're going
13 to really know about me and where I'm coming from and that's
14 how they identify me, but coming from my house.

10:01:34

15 So if I receive an e-mail from a victim from Gmail and
16 it has an IP address, 1234, I can search on the Internet and
17 find out what company that IP address is assigned to. So
18 that would come back and on the Internet and tell me this is
19 assigned to WOW Internet. It's not going to give my name on
20 the Internet. It's going to give the company. And I would
21 then send a subpoena to WOW Internet and say on this day at
22 this time, who was using IP address 1234.

10:01:53

23 **Q.** Okay.

10:02:11

24 So just as an example, let's say I sent a bomb threat
25 by Gmail by -- from Gmail. Could you use my IP address to

Diaz - Direct/Levine

1 help identify me?

2 **A.** Yes.

3 **Q.** And so how would that work?

4 **A.** Similar to the explanation I just gave, I would look
10:02:23 5 up your IP address, find out what company that providers
6 also provide is assigned to, such as Comcast. If you use
7 Comcast, I would then send a subpoena to Comcast and again
8 say this is the IP address that I'm interested in, this is
9 the date and the time, because they're temporary, they can
10:02:41 10 change. So I have to have a specific time period when the
11 IP address was being used. And they would then tell me that
12 it was assigned to you at your house at -- during that
13 particular time period.

14 **Q.** Let me throw a curve ball at you. What if I made this
10:02:57 15 bomb threat from Romania, say I was in Romania and my
16 computer in Romania and I make a bomb threat via Gmail.
17 What would you do?

18 **A.** If -- if it came back to a Romanian IP address, I
19 would then have to contact the Romanian authorities and they
10:03:15 20 would do something similar in their own legal process of
21 acquiring a subpoena in Romania to request the Internet
22 Service Provider in Romania to provide the records on that
23 IP address.

24 **Q.** Okay.
10:03:28 25 And would you do that typically by sending a subpoena

Diaz - Direct/Levine

1 or what is the legal process you would use if it was
2 Romania?

3 **A.** Right. For me to send the request to the Romanians, I
4 have to send what's called an M-LAT. It's Mutual Legal
10:03:41 5 Assistance Treaty. So I would send an M-LAT to Romania,
6 which is a legal document basically saying I would like for
7 you to do this for me, I would like this request. And they,
8 based on my M-LAT request, would get a subpoena, they -- the
9 equivalent of a subpoena in their legal system in Romania to
10:04:00 10 get the records on the IP address.

11 **Q.** Okay.

12 So now where in the e-mail -- because I've seen a lot
13 of e-mails. I have a never seen an IP address in an
14 e-mail -- where in the e-mail is the IP address?

10:04:12 15 **A.** The IP address is what's in -- what's called the
16 header information, which generally is not viewed when we
17 look at e-mail. All we see is to and from and the date and
18 the subject line.

19 If you go into the settings on your e-mail, you can
10:04:26 20 ask to display the full header information, and then it will
21 be shown to you. And inside the header information is a lot
22 of different information about the servers that the e-mails
23 are coming from and it will have in there the IP address.

24 **Q.** Okay.

10:04:40 25 So you sent out subpoenas and other process to these

Diaz - Direct/Levine

1 e-mail providers. What type of IP address information did
2 the providers send back to you?

3 **A.** I'm not sure I understand your question.

4 **Q.** So you testified earlier that one of the things the
10:04:56 5 providers give back to you in response to your subpoenas and
6 search warrants was IP address information.

7 What type of IP address information?

8 **A.** So they would provide an IP address for when the
9 account was created and then every time the account was
10:05:12 10 accessed by the user, they would have a log an IP address
11 log showing all the different IP addresses that were used by
12 the person accessing that e-mail account.

13 **Q.** Was the IP address information that you received from
14 the providers, was that useful in identifying the specific
10:05:31 15 members of the Bayrob Group?

16 **A.** Not the actual identities of the members of the Bayrob
17 Group, no.

18 **Q.** Why not?

19 **A.** Because the IP addresses generally were from the
10:05:40 20 United States and they were infected computers.

21 **Q.** Okay.

22 Now, I'd like to show you a demonstrative that has
23 been previously marked as Government's Exhibit 2037. If you
24 could bring that just up for us. Thank you so much.

10:06:00 25 THE COURT: Well, if it's demonstrative, you

Diaz - Direct/Levine

1 can just go ahead.

2 MR. LEVINE: Okay. Bring it up for everybody
3 then. Thank you. Thank you, your Honor. We're whipping
4 along.

10:06:12 5 Q. Okay. So without going -- without explaining the
6 demonstrative yet, Special Agent Diaz, what is this a
7 demonstrative of?

8 A. Explains what a proxy server is.

9 Q. Okay. And what -- would this demonstrative help you
10:06:30 10 to explain to the jury what a proxy is?

11 A. Yes.

12 Q. Okay.

13 Will you use this demonstrative please to help explain
14 what a proxy is and how that works.

10:06:40 15 A. A proxy server is used to mask your IP address. So as
16 we discussed earlier, if this is my house, and my IP address
17 given to me by WOW Internet is 1234, then I could connect to
18 what we call a proxy server, which is just another computer
19 on the Internet.

10:06:59 20 I use this proxy server to then change what appears to
21 be my IP address. The proxy server would then show up as
22 5678. So when I could connect to Gmail and send an e-mail,
23 my IP address would then appear to be 5678 instead of 1234.

24 Q. Okay.

10:07:20 25 So what -- so first of all, we see the word proxy

Diaz - Direct/Levine

1 there. Is proxy short for proxy server?

2 **A.** Yes.

3 **Q.** Okay. And what -- can you give us some examples of
4 what proxies might be?

10:07:34 5 **A.** So a lot of people use proxies legitimately. It
6 can -- it is a way for a group of computers to have the same
7 IP address. So AOL would actually have proxy servers
8 available and you can access their proxy server and use
9 their proxy servers without having to hack into it or use it
10:08:01 10 maliciously.

11 **Q.** All right.

12 So one example is America Online. What's another
13 example of a proxy?

14 **A.** So a lot of companies will have proxy servers
10:08:18 15 available. I believe Yahoo has proxy servers.

16 **Q.** Okay. You have mentioned earlier infected computers?

17 **A.** Yes, I'm sorry.

18 **Q.** Would infected computers -- could infected computers
19 act as proxies?

10:08:29 20 **A.** Yes, absolutely.

21 So the computers that were infected with the Bayrob
22 trojan were designed and set up to be able to be used as
23 proxy servers --

24 MR. GOLDBERG: Objection.

10:08:39 25 THE WITNESS: -- themselves.

Diaz - Direct/Levine

1 THE COURT: Overruled.

2 THE WITNESS: Sorry.

3 The infected computers themselves could be used as
4 proxy servers, too.

10:08:48 5 Q. Okay.

6 So can you explain what would happen and what did
7 happen when you tried to get IP address information from the
8 subscriber where a proxy server is used, as in the
9 demonstrative?

10:09:04 10 A. So if I had an e-mail from -- that was sent from
11 Gmail, then I would get the IP address of the proxy. And if
12 this is an infected computer with the Bayrob trojan, I could
13 then identify it as an infected computer, but it would not
14 be keeping track of where the original IP address was.

10:09:26 15 Q. Okay.

16 So is that why you weren't able to identify or strike
17 that? Does that explain why the IP addresses you got back
18 from these providers did not help you identify?

19 MR. O'SHEA: Objection.

10:09:44 20 THE COURT: Overruled. I'll allow that.

21 THE WITNESS: Yes.

22 So although we wouldn't receive IP addresses from
23 e-mail accounts and other websites the Bayrob Group was
24 using, all of these IP addresses would help us identify
10:09:58 25 infected computers with the Bayrob trojan. But once we got

Diaz - Direct/Levine

1 to that infected computer, there was no way for us to track
2 back further to get a true IP address of where the
3 individual was actually located.

4 Q. Okay.

10:10:13 5 So in this case, what type of computers and servers
6 were the Bayrob Group using as proxies? You mentioned
7 infected computers. Anything else?

8 A. As I mentioned, they would use proxy server at AOL.
9 They would also use VPN services.

10:10:30 10 Q. What's a VPN service?

11 A. It stands for Virtual Private Network, and this is a
12 company, multiple companies are available on the Internet.
13 You can pay for access to use their VPN service.

14 Q. Okay.

10:10:43 15 Is the VPN service the way people typically log in to
16 their company network remotely?

17 A. Yes.

18 Q. All right. So let's just take that hypothetical.

19 Let's say I log into the DOJ's network from home. And I
10:11:01 20 committed some crime there at the DOJ or Gmail or wherever I
21 went to. What IP address would you see in that instance?

22 A. I would see the IP address of the VPN.

23 Q. Not of the VPN, not my home IP address?

24 A. That is correct.

10:11:14 25 Q. Okay.

Diaz - Direct/Levine

1 So you said the Bayrob Group used America Online.

2 They used infected computers, and they used VPNs?

3 **A.** Yes.

4 **Q.** And you said VPN stands for Virtual Private Network?

10:11:27 5 **A.** Yes.

6 **Q.** Okay.

7 Now, did you communicate with America Online to see if
8 it was able to provide you with a true IP address for the
9 Bayrob Group?

10:11:38 10 **A.** Yes, we did.

11 **Q.** And was America Online able to provide you with the
12 true IP address?

13 **A.** No, they were never able to give us true IP addresses
14 either.

10:11:47 15 **Q.** Why was that?

16 **A.** Again, as we later determined, the Bayrob Group
17 members would jump through multiple proxy servers. So it
18 wasn't just they were going directly to AOL and then from
19 that point, going to somewhere else. They would jump
10:12:04 20 through at least three infected computers, then to AOL and
21 then maybe even to another VPN service after that, taking
22 multiple steps to hide their IP address.

23 **Q.** Okay.

24 So was there anything in the e-mails at all between
10:12:21 25 the victims and the Bayrob Group that helped you identify

Diaz - Direct/Levine

1 the particular members of the Bayrob Group?

2 **A.** No, there was not.

3 **Q.** Did you also follow the money that the victims wired
4 to purchase what they thought were cars?

10:12:35 5 **A.** Yes, I did.

6 **Q.** And how did you do that?

7 **A.** So the original victims would provide us with the bank
8 account information from where they sent the money
9 themselves, and we would -- I would follow up on that point,
10:12:51 10 following the money and get the bank records.

11 **Q.** Okay.

12 And how did you find the person that initially
13 received the money, the person the victim sent the money to?

14 **A.** So sometimes they would have -- the victim themselves
10:13:06 15 would already have the name of the person that they sent the
16 money to, but minimally, they would at least have the
17 bank -- the bank itself and then the bank account number
18 where they were wire transferring money.

19 **Q.** All right.

10:13:18 20 And who was it that received the money these victims
21 sent?

22 **A.** It was different people throughout the country and in
23 the United States.

24 MR. O'SHEA: Objection, Judge.

10:13:27 25 THE COURT: No, overruled.

Diaz - Direct/Levine

1 THE WITNESS: So there were people in the
2 United States that were acting as what we call money mules
3 for the Bayrob Group.

4 Q. Okay.

10:13:39 5 And what is a money mule? What does that mean? What
6 does that term mean to you?

7 A. A money mule is simply someone who is transporting
8 money from one location to another. It is similar to a drug
9 mule, which I think most people are more familiar with. A
10:13:55 10 drug mule picks up drugs from one location and takes it to
11 another location. A money mule either may pick up cash and
12 transport cash. In this -- in this example, they would
13 receive money into the bank. They would withdraw the money
14 in cash, and then transfer it where they were told to
10:14:12 15 transfer it.

16 Q. Okay.

17 So approximately how many US money mules did you and
18 the FBI colleagues speak with as part of the investigation
19 into the Bayrob Group?

10:14:23 20 A. We interviewed approximately 30 to 40 million.

21 Q. And approximately how many US money mules did you and
22 the colleagues obtain records from as part of your
23 investigation into the Bayrob Group?

24 A. Approximately about the same -- the same number,
10:14:40 25 around 40 money mules.

Diaz - Direct/Levine

1 Q. All right. And how were these money mules recruited?

2 A. The Bayrob Group members would post websites to be
3 able to recruit these money mules in the United States.

4 Q. Okay.

10:14:56 5 And did you discover websites? Did you discover these
6 websites?

7 A. Yes, we did. They would post advertisements on
8 websites, some of which were commercially available, such as
9 Indeed or monster.com, and also create their own websites to
10:15:15 10 post advertisements to hire these people.

11 Q. Okay. What is -- I'm not -- what is indeed.com?

12 A. Indeed.com is a job recruitment website, similar to
13 monster.com if you're familiar with monster.

14 Q. So both of these are places you could go look for a
10:15:34 15 job?

16 A. Yes.

17 Q. Okay.

18 So Bayrob Group would place ads. What would the ads
19 look like?

10:15:39 20 A. Oftentimes, the ads would say that they were looking
21 for someone who could be a transfer agent and would be
22 responsible for transferring money. But, they would also
23 frequently just post an ad that would advertise for some
24 other type of job, whether it be, you know, delivering cars
10:16:00 25 or moving cars. And then once they had you hooked in, then

Diaz - Direct/Levine

1 they would say okay, the real job is to be a transfer agent.
2 We want you to be a transfer agent.

3 Q. Okay.

4 And did you say -- did you discover other websites
10:16:13 5 associated with these postings besides the job websites?

6 A. Yes, we did.

7 Q. And what were those websites?

8 A. Their own website that they created with the names of
9 fictitious companies, such as KPL, ITP, all these different
10:16:29 10 companies that they made up and created websites for them.

11 Q. And did you investigate -- and we'll go through these
12 terms in a minute, but did you investigate who registered
13 the domains for these websites?

14 A. Yes, I did.

10:16:44 15 Q. Okay. So what is a domain?

16 A. A domain is the URL for a website, the name of the
17 website, such as CNN.com, that is a domain. Yahoo.com is a
18 domain.

19 Q. What does it mean to register a domain?

10:17:00 20 A. Anyone can go online and create your own domain. If I
21 want to, I can create Stacy Diaz, assuming it's not already
22 taken. I can make StacyDiaz .com and could go to Yahoo or
23 there's tons of other different registration websites online
24 to be used. And I can pay a fee and then I can register
10:17:21 25 StacyDiaz.com.

Diaz - Direct/Levine

1 Q. Okay.

2 So did investigating, who registered the domains for
3 those websites that KPL, ICP? Did that help you identify
4 any specific members of the Bayrob Group?

10:17:35 5 A. No, it did not.

6 Q. Okay. Why not?

7 A. Because they would use fake information. Again --

8 MR. O'SHEA: Objection.

9 THE COURT: Overruled.

10:17:45 10 THE WITNESS: They would register the domains
11 with someone else's name, and information, and credit card.

12 Q. Okay.

13 And did you identify -- did you investigate who paid
14 for those websites to be hosted?

10:17:58 15 A. Yes.

16 Q. And did that help you identify any members of the
17 Bayrob Group?

18 A. No, it did not.

19 Q. Okay.

10:18:03 20 And I guess step back. What does it mean to pay for
21 websites to be hosted?

22 A. Again, when you -- you pay to register the domain, and
23 then you can pay to have that website provided by Yahoo.com.

24 So again, if I wanted to create StacyDiaz.com, I could
10:18:25 25 pay to register that domain and could also pay Yahoo or some

Diaz - Direct/Levine

1 other hosting company to let me keep my website on their
2 server.

3 **Q.** Okay.

4 So did -- looking for who paid for those websites to
10:18:40 5 be on Yahoo server, whoever's server, did that help you
6 identify any members of the Bayrob Group?

7 **A.** No, it didn't.

8 **Q.** And why not?

9 **A.** Because they would use someone else's identity,
10:18:52 10 someone else's name, someone else's credit card.

11 MR. O'SHEA: Objection.

12 THE COURT: Sustained -- I mean overruled. I
13 apologize.

14 **Q.** Okay. Can you just give your answer?

10:19:01 15 THE COURT: I'm assuming it's the same basis
16 for all of your objections.

17 MR. O'SHEA: Yes.

18 BY MR. LEVINE:

19 **Q.** Okay.

10:19:05 20 Can you give your answer again so it's clear on the
21 record?

22 **A.** Yes. So when they would pay Yahoo to host these
23 domains, they would use someone else's information, someone
24 else's name, address, and credit card.

10:19:18 25 **Q.** All right.

Diaz - Direct/Levine

1 And I'd like to bring up for us now what has been
2 previously marked as Government's Exhibit 1893 -- sorry.

3 THE COURT: Sorry.

4 MR. LEVINE: 1893.

10:19:39 5 THE JURY: We see it on our screen.

6 MR. LEVINE: Thank you for letting me know
7 that. Just for us here. But, it's not on our screen.

8 THE COURT: You need to be specific for me.

9 MR. LEVINE: Oh, I'm sorry, your Honor.

10:19:49 10 THE COURT: That's all right.

11 MR. LEVINE: So we'd like to see it just on
12 our screen, not on theirs. Okay. Perfect. Thank you.

13 BY MR. LEVINE:

14 Q. All right.

10:19:58 15 So, Special Agent Diaz, what is Government's Exhibit
16 1893 there?

17 A. This is an example of an agreement for a money mule
18 with one of the companies that the Bayrob Group used.

19 Q. Okay. How did you obtain -- how do you obtain
10:20:16 20 Government's Exhibit 1893?

21 A. We interviewed the person, Articia Harrison, who was
22 acting as a money mule for the Bayrob Group.

23 MR. O'SHEA: Objection.

24 THE COURT: Well, sustained.

10:20:30 25 Q. Well, the question is how she obtained it. I think

Diaz - Direct/Levine

1 you answered that but let's get it clear on the record.

2 THE COURT: Wait. Sustained.

3 MR. LEVINE: Okay.

4 Q. So how did you -- so without saying what anybody told
10:20:43 5 you, how did you obtain Government's Exhibit 1893?

6 A. Articia Harrison provided a copy of.

7 MR. O'SHEA: Objection.

8 THE COURT: Finish your answer, ma'am.

9 Provided it to?

10:20:57 10 THE WITNESS: To the FBI.

11 THE COURT: To you?

12 THE WITNESS: Not to me directly, to someone
13 else from the FBI.

14 THE COURT: Do a follow-up.

10:21:10 15 BY MR. LEVINE:

16 Q. Okay.

17 And then how did you obtain it -- well, let me step
18 back for a moment.

19 You testified earlier that you interviewed a
10:21:19 20 significant number of money mules that were US based; is
21 that correct?

22 A. Yes, that is correct.

23 Q. Okay.

24 And when you interviewed those money mules, you also
10:21:26 25 testified that you obtained documents from them?

Diaz - Direct/Levine

1 **A.** Yes.

2 **Q.** Is this one of the documents that you obtained from
3 money mules that were interviewed?

4 **A.** Yes.

10:21:35 5 **Q.** Okay.

6 Does Government's Exhibit 1893 contain a fair and
7 accurate copy of the wire transfer, some of the wire
8 transfer applications that you obtained from US money mules?

9 **A.** Yes, it does.

10:21:48 10 **Q.** Okay.

11 MR. LEVINE: Your Honor, I'd like to move to
12 admit Government's Exhibit 1893.

13 MR. O'SHEA: Side bar on this, your Honor?

14 THE COURT: You may.

10:21:59 15 (The following proceedings were held at side bar:)

16 MR. O'SHEA: 1839 is more of -- sorry, Judge.
17 1893 is more than just this service agreement. It's -- if
18 I'm not mistaken, guys, it's got some e-mails contained in
19 it, some communications back and forth. So it's -- you
10:22:31 20 know, I -- I don't necessarily have a problem with
21 publishing to the jury the agreement that you got, but the
22 other stuff, guys, I don't think it's fair.

23 MR. LEVINE: I just move to publish it right
24 now because we're doing all the admission at the end. I
10:22:49 25 understand.

Diaz - Direct/Levine

1 But these are all -- they all fit into hearsay
2 exceptions in our motion. They are -- your Honor --

3 THE COURT: But if you recall, I said I have
4 to look at every document to determine if it's hearsay
10:23:07 5 within hearsay. We've been over there so many times, folks.

6 MR. LEVINE: Your Honor, I presented -- we
7 presented all of them in advance to the Court with the
8 hearsay motion explaining what our position was.

9 THE COURT: What was my order?

10:23:22 10 MR. LEVINE: Your order was to do it in court
11 and that's -- so, yeah but --

12 THE COURT: Because I'm going to say it again.
13 How can I possibly say 1,000 exhibits I'm going to let them
14 all in without looking at them? I can't do that.

10:23:41 15 MR. LEVINE: So, your Honor, with respect to
16 this particular exhibit, I am just going to ask Stacy Lough,
17 Stacy Diaz, whether she investigated the information that
18 was in --

19 THE COURT: It's not what you asked. So tell
10:23:57 20 me what you -- what you want the jurors to see right now so
21 Mr. O'Shea and Mr. Goldberg can say if they have a problem
22 with a portion of it being shown.

23 MR. LEVINE: I'm just going to ask -- I'm
24 going to ask what personal information did prospective money
10:24:16 25 mules have to provide to the Bayrob Group, and then did she

Diaz - Direct/Levine

1 investigate -- did she -- you know, go through all the
2 investigative steps with respect to that information and did
3 that help identify the Bayrob Group. That's basically what
4 we're going to --

10:24:34 5 MR. O'SHEA: Okay. I'm looking at Exhibit
6 Number -- what number are we guys? Sorry. Give me a
7 second. 1893, right?

8 MR. LEVINE: Yes.

9 MR. O'SHEA: All right. It's eight pages
10:24:43 10 long. The first four pages are the service agreement. The
11 other four pages, I think --

12 THE COURT: I'm going to stop you.

13 Folks, we're going to talk at a break. This can't go
14 on. We have got to figure this out because you've got
10:25:00 15 thousands and thousands and thousands of exhibits up here.
16 We can't do this for each exhibit. You ask the question, "I
17 want to publish it to the jury." Well that tells me the
18 entire exhibit you want published to the jury. Now I'm
19 hearing, "Wait a minute, Judge. There's hearsay in there."
10:25:20 20 You need to look at this document before it's published."
21 So you need to figure out how we're going to do this without
22 coming to side bar for every exhibit.

23 MR. LEVINE: Okay.

24 So perhaps what we can do at the beginning of the day
10:25:35 25 is to give you a copy of the exhibits we're going to be

Diaz - Direct/Levine

1 using that day.

2 MR. O'SHEA: How about the night before?

3 THE COURT: I'm not going to let you publish
4 it. Let's go.

10:25:49 5 (Proceedings resumed within the hearing of the jury:)

6 BY MR. LEVINE:

7 Q. Okay. Thank you, your Honor.

8 Looking at Government's Exhibit 1893, what personal
9 information did prospective wire transfer agents have to
10:26:12 10 provide to the Bayrob Group?

11 A. They had to provide their bank account, the bank
12 address, the bank name, the routing number, and their bank
13 account number.

14 Q. Okay.

10:26:25 15 And at one point, did you personally apply to become
16 an agent for the Bayrob Group?

17 A. Yes, I did.

18 Q. Why did you do that?

19 A. I was hoping to see if that was a way that I could
10:26:40 20 lead to information that would identify the Bayrob Group
21 members.

22 Q. Okay.

23 And did you fill out one of these wire transfer
24 applications and submit it to the Bayrob Group?

10:26:49 25 A. Yes, I did.

Diaz - Direct/Levine

1 Q. Were you ever selected by the Bayrob Group to become a
2 wire transfer agent?

3 A. No, I wasn't.

4 Q. Do you know why you weren't selected?

10:26:57 5 A. No, I don't know why.

6 Q. Did you use a real identity in the application?

7 A. No, I didn't.

8 Q. You didn't tell them you were with the FBI, did you?

9 A. No, I did not.

10:27:06 10 Q. Okay.

11 So if a person were hired to be a transfer agent for
12 the Bayrob Group, what would happen?

13 A. Well, they would communicate with the Bayrob Group
14 primarily through e-mail. Sometimes through instant
10:27:20 15 messaging and be instructed when they were going to receive
16 wire transfers into their bank account and where they were
17 supposed to transfer that money to.

18 Q. And you said -- the Bayrob Group used e-mail to
19 communicate with the wire transfer agents?

10:27:36 20 A. Yes.

21 Q. Did they communicate with any -- any other method?

22 A. As I mentioned, sometimes in instant messaging as
23 well.

24 Q. Okay.

10:27:44 25 Let -- if you could please bring up what's been marked

Diaz - Direct/Levine

1 as Government's Exhibit 1322. And we're not publishing this
2 to the jury yet. 1322.

3 Okay. What is Government's Exhibit 1322?

4 **A.** This is an e-mail provided to me by Read Notify.

10:28:10 5 **Q.** And from where -- oh, you just answered that. Okay.

6 And is Government's Exhibit 1322 a fair and accurate copy of
7 a Read Notify e-mail as it was produced to you by Read
8 Notify?

9 **A.** Yes, it is.

10:28:22 10 **Q.** Okay.

11 So I would like to publish Government's Exhibit 1322,
12 subject to the prior caveats that we discussed.

13 MR. GOLDBERG: Objection.

14 THE COURT: I will not permit it to be
10:28:36 15 published then.

16 **Q.** Okay. At a general level, who is this e-mail between?

17 **A.** Can I see the hard copy of it?

18 MR. LEVINE: Yes.

19 THE WITNESS: Thank you. There's an e-mail
10:29:12 20 between a Bayrob Group member and a potential money mule.

21 **Q.** And who is the sender of the ultimate e-mail there?

22 **A.** It came from an e-mail address named
23 m.kleinberg@KPL-business.com.

24 **Q.** And is there anything significant to you about that
10:29:32 25 name, e-mail address?

Diaz - Direct/Levine

1 **A.** Well, a couple things. KPL is one of the names of the
2 fictitious companies that the Bayrob Group would use to
3 recruit money mules. And then m.kleinberg was one of the
4 names that they frequently used, stands for -- Martin
10:29:52 5 Kleinberg was a name that we saw a lot in communication with
6 money mules.

7 **Q.** Okay.

8 And looking towards the bottom of Page 2 on to Page 3,
9 can you summarize what Martin Kleinberg's is saying in this
10:30:11 10 e-mail?

11 MR. O'SHEA: Objection.

12 MR. GOLDBERG: Objection.

13 THE COURT: Folks, we are going to take a
14 recess so that we can address some legal issues outside of
10:30:24 15 your hearing. Remember the admonition.

16 All rise for the jury.

17 (Proceedings in the absence of the jury:)

18 THE COURT: You may continue, Mr. Levine.

19 MR. LEVINE: Thank you, your Honor.

10:43:28 20 **Q.** Thank you for that break. All right.

21 We were looking at Government's Exhibit 1322, which
22 you indicated was an e-mail between a potential money mule
23 and a member of the Bayrob Group.

24 Special Agent Diaz, could you please read what the
10:43:43 25 Bayrob Group member says to the potential money mule?

Diaz - Direct/Levine

1 **A.** Which part? Do you want me to read the very last
2 e-mail?

3 **Q.** It begins at the bottom of Page 1 of Government's
4 Exhibit 1322 and goes on to the next page.

10:44:04 5 **A.** Okay.

6 So he says, "Darryl, what is your phone number? Let
7 me first start by saying I understand your concern. You ask
8 yourself would these folks have access to my bank account.
9 No, we won't. This isn't possible as we can use the bank
10:44:17 10 account information only to get money routed to you. We
11 cannot use in any other way.

12 "As you noticed, my name is Martin Kleinberg, and I am
13 in charge of your application in case you decide to join us.
14 Once I validate it, you will only be dealing with me here at
10:44:33 15 KPL. We will keep in touch, mainly per e-mail. Should
16 something urgent come up, I will call you at the phone
17 number you have provided. I understand you registered and
18 you need income. Let me be straight with you. This is not
19 going to be a steady income. This is a commission-based
10:44:51 20 job. So you will earn a commission.

21 "I cannot predict the monthly number of transactions.
22 It will be a couple of weeks until you get your first
23 because this time of year is very crowded. And we have many
24 I'm not sure, partners, like you, are already waiting.
10:45:06 25 However, once the first transaction is assigned, others are

Diaz - Direct/Levine

1 more likely to follow. The usual rate is two to three per
2 week.

3 "Let me explain what you'll have to do when it all
4 starts. We'll take a transfer to your account and once it
10:45:21 5 is posted, you will have to withdraw the funds and send it
6 to our client via Western Union. We support the Western
7 Union fees. So you will deduct these from the received
8 amount. And you will have to choose whatever you prefer, a
9 10 percent commission, which will be paid via certified
10:45:38 10 check, or you can opt for a 6 percent immediate payment,
11 which means that you get to keep 6 percent of the received
12 amount as soon as you withdraw it.

13 "I'm looking forward to receiving your application
14 either an old or a new bank account, what you feel will suit
10:45:52 15 best. Regards, Martin Kleinberg."

16 **Q.** All right. Thank you, Special Agent Diaz.

17 Now given that the Bayrob Group used Read Notify to
18 communicate with money mules, did you analyze the Read
19 Notify e-mails to try to identify victims and trace
10:46:10 20 proceeds?

21 **A.** Yes, I did.

22 **Q.** And I'd like to bring up, just for us, Government's
23 Exhibit 1869.

24 What is Government's Exhibit 1869?

10:46:24 25 **A.** This is a spread sheet showing data that was taken

Diaz - Direct/Levine

1 from e-mails provided to me by Read Notify.

2 Q. Okay.

3 And what specifically is it analyzing?

10:46:46

4 A. This shows data from Western Union transfers from
5 money mules in the United States to money mules receiving
6 them in Europe, and it also details for most of them the
7 victim that ultimately, that initially sent the money to the
8 money mule in the United States.

9 Q. Okay. And who prepared this spread sheet?

10:47:02

10 A. I did.

11 Q. All right.

12 And does Government's Exhibit 1869 fairly and
13 accurately reflect information you obtained regarding the
14 victim's wire transfers taken solely from Read Notify
15 e-mails?

10:47:15

16 A. Yes, it does.

17 Q. Are the underlying e-mails from which this spread
18 sheet was created too voluminous and complex for the jury to
19 reasonably look at during trial?

10:47:27

20 MR. O'SHEA: Objection to the form of the
21 question.

22 THE COURT: Overruled.

23 THE WITNESS: Yes.

24 Q. Okay. Let me just ask it again just so it's clear on
25 the record.

10:47:32

Diaz - Direct/Levine

1 Are the underlying e-mails from which the spread sheet
2 was created too voluminous and complex for the jury to
3 reasonably review at trial?

4 MR. O'SHEA: Same objection.

10:47:41 5 THE COURT: Overruled. It's an evidentiary
6 issue.

7 THE WITNESS: Yes, there are over 19,000
8 e-mails.

9 Q. Okay.

10:47:48 10 MR. LEVINE: Your Honor, a copy of
11 Government's Exhibit 1869 and the underlying Read Notify
12 e-mails have all been made available to Defense as part of
13 discovery. All the Read Notify e-mails are statements in
14 furtherance of the conspiracy and, therefore, not hearsay
10:48:01 15 as --

16 MR. O'SHEA: Objection.

17 THE COURT: Yes. No statements in front of
18 the jury. Sustained.

19 MR. LEVINE: Okay.

10:48:08 20 And there are no statements in the spread sheet, your
21 Honor.

22 MR. O'SHEA: Objection.

23 THE COURT: Sustained.

24 No statements will be allowed in front of the jury.
10:48:17 25 Folks, disregard all of the statements just made.

Diaz - Direct/Levine

1 MR. LEVINE: Okay.

2 Q. So based on your analysis that you completed in this
3 spread sheet, how much victim funds were you able to trace
4 just using the Read Notify e-mails?

10:48:35 5 A. At the bottom of the exhibit, it shows a total of over
6 \$2 million.

7 Q. Okay. \$2 million and what?

8 A. \$2,100,000.

9 Q. Okay.

10:48:47 10 And does that -- does that -- you need to look at the
11 actual -- there you go. What was the total?

12 A. The total is \$2,194,636.11.

13 Q. Okay.

14 And does that approximately 2.2 million represent a
10:49:07 15 total amount of victim loss that you were able to quantify
16 or just those based on Read Notify e-mails?

17 A. These are just ones from Read Notify.

18 Q. Okay.

19 Was the approximate total amount of victim loss just
10:49:20 20 from eBay fraud that you were able to quantify?

21 MR. O'SHEA: Objection.

22 THE COURT: Overruled.

23 THE WITNESS: The total that we were able to
24 identify and associate to the Bayrob Group is approximately
10:49:31 25 \$4 million.

Diaz - Direct/Levine

1 Q. And did you investigate the e-mail accounts we just
2 talked about that the Bayrob Group used to communicate with
3 money mules?

4 A. Yes, I did.

10:49:42 5 Q. And did that help you identify any members of the
6 Bayrob Group?

7 A. No, it did not.

8 Q. Why not?

9 A. When they would register the e-mail account, they
10:49:52 10 would use fake information, a fake name, and fake address,
11 and then as we talked about earlier, whenever they would
12 send e-mails, they were going through at least one proxy
13 server to hide their IP address.

14 Q. Okay.

10:50:08 15 So at a general level, once a wire transfer agent or a
16 money mule received a transfer of money to their account,
17 what was he or she supposed to do with it?

18 A. The money mules were instructed to withdraw the money
19 out of their bank account in cash, and then go to Western
10:50:26 20 Union and transfer the money overseas via Western Union.

21 Q. Okay. And where in overseas were they instructed to
22 send it?

23 A. The transfers were received in multiple different
24 countries. And initially in the beginning of the
10:50:42 25 investigation, most of the transfers were received in

Diaz - Direct/Levine

1 Greece. They would move over time to Hungary to Romania to
2 Bulgaria, multiple different countries in that geographic
3 location part of Europe.

4 **Q.** Okay.

10:50:56 5 Did you send legal process to Western Union to find
6 out where the money was transferred and who picked it up?

7 **A.** Yes, I did.

8 **Q.** What information were you able to obtain back from
9 Western Union?

10:51:06 10 **A.** They would provide me words on each individual
11 transaction. Showing who received the money based off an ID
12 that person would present when they would receive the money.
13 How much money that they were picking up and where the
14 Western Union location was located that they went to.

10:51:24 15 **Q.** And with respect to the people picking up the money
16 from Western Union, what country was the driver's license
17 usually from?

18 **A.** Usually from Romania.

19 **Q.** And did you find that fact significant to your
10:51:35 20 investigation?

21 **A.** Yes.

22 It gave me a clue that the people that were part of
23 the Bayrob Group might possibly be from Romania.

24 **Q.** All right.

10:51:46 25 And did you investigate the identity of the people

Diaz - Direct/Levine

1 picking up the Western Unions in Europe?

2 **A.** Yes, I did.

3 **Q.** How did you investigate the identity of the people
4 picking up the Western Unions in Europe?

10:51:58 5 **A.** I provided all of the identification, the name and the
6 driver's license numbers to the FBI office that's located in
7 Bucharest, Romania.

8 **Q.** Where is that, is there an FBI office located in
9 Bucharest, Romania?

10:52:14 10 **A.** Yes, there is.

11 **Q.** Why is that?

12 **A.** Most countries throughout the world have an FBI
13 agent -- FBI office that is there to work with the local
14 authorities. Some offices cover multiple different
10:52:31 15 countries. So not necessarily one in every single country
16 throughout the world, but we have one that is for each
17 country. So there is an office in the US Embassy in
18 Bucharest, Romania.

19 **Q.** All right. And who -- what is a LEGATT?

10:52:45 20 **A.** The LEGATT stands for -- the LEGATT -- the Legal
21 Attache, which is the supervisor, FBI Special Agent in the
22 LEGATT office in that country.

23 **Q.** So there's a LEGATT in the FBI office in Romania?

24 **A.** Yes, there is.

10:53:03 25 **Q.** And what's an ALATT, just so we have all these terms

Diaz - Direct/Levine

1 out here?

2 **A.** An ALATT is the Assistant Legal Attache. So there's
3 the supervisor, and then there could be multiple Special
4 Agents working underneath that supervisor.

10:53:16 5 **Q.** Now in 2007, how many full-time FBI employees did the
6 FBI have in Romania?

7 **A.** There was one full-time FBI agent and then there was
8 at times one other person that would come in and spend a
9 little bit of time assisting.

10:53:33 10 **Q.** And now how many FBI, full-time FBI are there in
11 Romania?

12 MR. O'SHEA: Objection.

13 THE COURT: Overruled.

14 THE WITNESS: There are approximately six FBI
10:53:42 15 agents full-time in Bucharest, Romania, at all times.

16 **Q.** Okay.

17 So when you got this identity information for the
18 Western Union, now that we know these people, who did you
19 send it to at the FBI in Romania?

10:53:58 20 **A.** So I would send it to, most of the time, the ALATT if
21 there was one. Initially it was the LEGATT that was working
22 there, and then as the office increased, I would work
23 directly with one of the ALATTs there. So I would send the
24 information for the ID's that were picking up Western Unions
10:54:14 25 to the LEGATT office.

Diaz - Direct/Levine

1 Q. And what did you determine about the identity of the
2 people picking up the Western Unions in Europe?

3 A. The LEGATT was able to request --

4 MR. GOLDBERG: Objection.

10:54:28 5 THE COURT: Go ahead, ma'am.

6 THE WITNESS: The LEGATT was able to determine
7 that all of the ID's --

8 THE COURT: Well, sustained.

9 THE WITNESS: Okay.

10:54:38 10 BY MR. LEVINE:

11 Q. Did having the LEGATT investigate the identity of the
12 money mules in Europe help you identify any members of the
13 Bayrob Group?

14 A. No, it did not.

10:54:53 15 Q. And why not?

16 A. All of the ID's --

17 MR. GOLDBERG: Objection.

18 THE COURT: No. Go ahead, ma'am.

19 THE WITNESS: All of the ID's that were used,
10:55:03 20 all of the driver's licenses that were used to pick up
21 Western Unions were all fake driver's licenses.

22 THE COURT: Sustained. That will be stricken.

23 BY MR. LEVINE:

24 Q. Okay.

10:55:13 25 But, none of the information provided back to you from

Diaz - Direct/Levine

1 the FBI -- or let me open that up.

2 Was any of the information provided back to you from
3 the LEGATT about the European money mules useful in helping
4 you identify any members of the Bayrob Group?

10:55:27 5 **A.** No, it was not.

6 **Q.** All right.

7 Did the FBI consider having someone surveil the
8 Western Unions in Europe or wait there for money mules to
9 pick up the wires?

10:55:37 10 **A.** Yes, we did.

11 **Q.** And did you try that?

12 **A.** We were not able to.

13 **Q.** Why not?

14 **A.** The money mules that were picking up all the transfers
10:55:47 15 for the Bayrob Group would always go to a different --

16 MR. O'SHEA: Objection.

17 THE COURT: Overruled. Go to a different
18 what?

19 THE WITNESS: To a different Western Union
10:55:58 20 location.

21 THE COURT: Overruled.

22 THE WITNESS: So the same Western Union
23 location was not used all the time. So I did not know
24 exactly where the wire was going to be picked up. And that
10:56:13 25 would complicate things because when you send money to a

Diaz - Direct/Levine

1 particular person in Romania, that person can pick up the
2 wire at any location of any Western Union location
3 throughout all of Romania. It doesn't have to be in a
4 specific city or a specific town. It can be anywhere in
10:56:32 5 that country.

6 And since I did not know the exact Western Union
7 location that the money mule was going to go to, we were not
8 able to do surveillance at every single Western Union
9 location in Romania.

10:56:45 10 **Q.** All right.

11 And how were the wire transfer agents or US money
12 mules supposed to be compensated by the Bayrob Group?

13 **A.** So they could pick one of two ways. They could get a
14 10 percent commission, but to do that, they had to send all
10:57:00 15 of the money through as instructed, and then they were told
16 they would receive a check back, a certified check in the
17 mail for 10 percent of their commission or they could choose
18 to keep 6 percent right away, deduct that out of the money
19 that they received, and then transfer the rest of it.

10:57:18 20 **Q.** So were you able to trace the source of the 10 percent
21 that came back from the Bayrob Group?

22 **A.** No.

23 **Q.** Why not?

24 **A.** There was no 10 percent that ever came back. The
10:57:31 25 money mules would never actually receive --

Diaz - Direct/Levine

1 MR. O'SHEA: Objection.

2 THE WITNESS: -- a certified checked.

3 THE COURT: Overruled.

4 Q. So the money mules were then victimized as well?

10:57:38 5 MR. O'SHEA: Objection.

6 THE COURT: Sustained.

7 Q. How else would the money mules be adversely impacted
8 by working for the Bayrob Group?

9 A. Several of the money mules were also victimized by the
10:57:51 10 fact that once they would receive the transfer into their
11 bank account, they would take the money out and immediately
12 send it to West Virginia. There were times when their bank
13 would determine that the transfer in was from a fraudulent
14 online auction. And they would actually refund the money
10:58:09 15 back to the victim so the victim would be made whole, would
16 get their money back, and the money mule would be stuck
17 owing their bank 8 to \$9,000.

18 Q. Okay. Any other negative impact?

19 A. Yes.

10:58:24 20 So they would also have their banks closed. Usually
21 one money mule would only last maybe two or three months
22 most of the time because the banks would start getting
23 notified that these transfers --

24 THE COURT: Overruled. Go ahead.

10:58:37 25 THE WITNESS: -- that the transfers coming in

Diaz - Direct/Levine

1 were from online auction frauds. So the bank accounts would
2 get closed. A lot of times, their credit would take a hit
3 because they end up owing money.

4 MR. O'SHEA: Objection.

10:58:49 5 THE COURT: Overruled.

6 THE WITNESS: So they might end up owing money
7 themselves. So they would be in debt to the bank and their
8 credit would go down and their bank accounts would get
9 closed.

10:58:58 10 Q. And were some of the mules prosecuted?

11 A. Yes, some of them are.

12 MR. O'SHEA: Objection.

13 THE COURT: Overruled.

14 Q. Did any of the money mules have any information at all
10:59:10 15 that was helpful in identifying the Bayrob Group?

16 A. No, they did not.

17 Q. Why not?

18 A. Because they were communicating primarily via e-mail.
19 All that they knew was they had this e-mail address and this
10:59:23 20 name, Martin Kleinberg, or one of the other names that they
21 used. And then as I said, if they used instant messaging,
22 all they had was the instant message account that they
23 communicated with.

24 Q. So just to be clear, who was Martin Kleinberg?

10:59:38 25 A. Martin Kleinberg was a made up name the Bayrob Group

Diaz - Direct/Levine

1 used. There were multiple names that we saw that were used
2 significantly.

3 Yojan Mayor is another name we see a lot. Claus.
4 Steinberg is another name that we saw a lot. They were just
10:59:56 5 made up names that they used.

6 **Q.** Okay.

7 So is it a fair summary of your testimony so far to
8 say that any time you investigated an e-mail address, an IP
9 address, an identity, a credit card number, or wire
11:00:07 10 transfer, or anything else to identify the Bayrob Group, it
11 all led to a dead end?

12 **A.** That is correct.

13 **Q.** And how long did it go on like this that you were
14 investigating all these Bayrob e-mail victims but hitting
11:00:19 15 into a brick wall in terms of identifying the Bayrob Group?

16 **A.** So until approximately 2013 -- so that is almost seven
17 years. Is that right?

18 **Q.** Well, it's 2007 to 2013, five or six?

19 **A.** Five or six years.

11:00:34 20 **Q.** Okay.

21 Were you -- were you actively investigating the Bayrob
22 Group that entire time?

23 **A.** Yes, I was.

24 **Q.** And based on your investigation, was the Bayrob Group
11:00:43 25 defrauding people during that entire time?

Diaz - Direct/Levine

1 MR. O'SHEA: Objection.

2 THE COURT: Sustained.

3 Q. Were you identifying new victims during that entire
4 time?

11:00:52 5 A. Yes, I was.

6 Q. So what was the first big break in the case?

7 A. In 2013, myself and other FBI members, we traveled to
8 California, and we met with eBay. We also met with
9 Symantec. And soon thereafter, we also went to Virginia and
11:01:13 10 met with AOL.

11 Q. So we're going to hear from America Online and
12 Symantec shortly, but fair to say information provided by
13 America Online and Symantec helped the FBI eventually
14 identify the Defendants sitting here today?

11:01:28 15 MR. O'SHEA: Objection.

16 THE COURT: Overruled. You may answer that.

17 THE WITNESS: Yes, that is correct.

18 Q. Okay.

19 And is it fair to say that you anticipate other
11:01:37 20 witnesses will be testifying regarding the identification of
21 the Defendants?

22 A. Yes.

23 Q. All right.

24 So what I want to do right now is fast forward in time
11:01:46 25 until May 14th, 2015. Okay? And did something significant

Diaz - Direct/Levine

1 to the Bayrob investigation happen on May 14, 2015?

2 **A.** Yes, it did.

3 **Q.** What happened on May 14, 2015?

4 **A.** Tiberiu Danet traveled to the United States.

11:02:06 5 **Q.** Okay.

6 From where did Tiberiu Danet travel to the United
7 States?

8 **A.** From Romania.

9 **Q.** And on May 14, 2015, had the FBI identified Tiberiu
11:02:16 10 Danet as the likely member of the Bayrob Group?

11 **A.** Yes, we had.

12 **Q.** Did the FBI know in advance that Danet was traveling
13 to the United States?

14 **A.** Yes. We were notified approximately, I think ten days
11:02:28 15 before he got here.

16 **Q.** How did the FBI have advanced notice?

17 **A.** The Romania authorities had notified --

18 MR. O'SHEA: Objection.

19 THE COURT: Sustained.

11:02:39 20 **Q.** So based on the information provided to you, where was
21 Danet planning to land in the United States on May 14, 2015?

22 **A.** Miami International Airport in Miami, Florida.

23 **Q.** And what was the FBI's plan for what you were going to
24 do when Danet landed?

11:02:56 25 **A.** We were going to have the Customs and Immigration

Diaz - Direct/Levine

1 department stop Danet and do a secondary search of him. And
2 during that time, we were going to also search his phones or
3 computers or anything that he had with him.

4 Q. Okay.

11:03:17 5 You mentioned the word secondary. What is -- what are
6 you referring to there?

7 A. So if you've been through customs before and this
8 country or another country, the border and customs agents
9 can decide that they would like to do an interview with you.
11:03:34 10 So you'll be a secondary interview, and so they will pull
11 you aside into a different room and then ask you some
12 questions. And during that time is when we were going to
13 search his items.

14 Q. Before Danet landed in Miami, did the FBI obtain a
11:03:53 15 search warrant to make an image copy of Danet's cellphone?

16 A. Yes, we did.

17 Q. And were you -- were you hoping to image Danet's
18 cellphone secretly in the sense that you didn't want Danet
19 to know that you were doing it?

11:04:06 20 A. Yes, that is correct.

21 Q. Why did you want to do it secretly?

22 A. We did not want him or any of the other Bayrob Group
23 members to know that we were investigating them.

24 Q. Okay.

11:04:18 25 So where were you located when Danet landed and was

Diaz - Direct/Levine

1 taken into a secondary?

2 **A.** I was in a conference room that was in the back area
3 of the airport.

4 **Q.** And what airport was that again?

11:04:34 5 **A.** Miami International Airport.

6 **Q.** And who else was in this conference room with you?

7 **A.** There were approximately, I think, 20 FBI people in
8 the room.

9 **Q.** Okay. Like who?

11:04:48 10 **A.** So myself and Special Agent Ryan MacFarlane were
11 there. There were, I believe, four or five computer
12 forensics examiners from the Miami FBI division, and then we
13 had -- we also had some other Special Agents from the Miami
14 division there to assist with surveillance, and then there
11:05:09 15 was approximately, I think, maybe five or six other FBI
16 employees from headquarters in Washington, D.C.

17 **Q.** And were there members of CBP, Customs and Border
18 Patrol as well?

19 **A.** Yes, there was.

11:05:21 20 **Q.** So in total, how many people were in the conference
21 room?

22 **A.** I think there was roughly 20 to 25 people.

23 **Q.** And is that standard FBI practice to have so many
24 people involved in an operation like this?

11:05:32 25 **MR. O'SHEA:** Objection.

Diaz - Direct/Levine

1 THE COURT: Sustained.

2 Q. Did you see Danet's cellphone the night of May 14,
3 2015?

4 A. Yes, I did.

11:05:39 5 Q. When was the first time you saw Danet's cellphone that
6 night?

7 A. The Customs and Border Patrol agent brought the
8 cellphone into the room to us.

9 Q. Okay. And that was the first time you saw it?

11:05:51 10 A. Yes.

11 Q. And I'd now like to bring up what is Government's
12 Exhibit 382 for us.

13 MR. LEVINE: Any objections to this being
14 published to the jury?

11:06:14 15 MR. O'SHEA: No objection.

16 MR. LEVINE: Okay.

17 Your Honor, I'd like to publish Government's Exhibit
18 382 to the jury.

19 MR. O'SHEA: No objection, Judge.

11:06:22 20 MR. GOLDBERG: No objection.

21 Q. Special Agent Diaz, what is Government's Exhibit 382?

22 A. This is the cellphone that was in the possession of
23 Tiberiu Danet on that night in question in May of 2015.

24 Q. And is Government's Exhibit 382 a fair and accurate
11:06:42 25 photograph of Tiberiu Danet's cellphone that was imaged on

Diaz - Direct/Levine

1 May 14, 2015?

2 **A.** Yes, it is.

3 MR. LEVINE: I move to admit Government's
4 Exhibit 382.

11:06:53 5 THE COURT: Will be admitted.

6 MR. LEVINE: Okay.

7 BY MR. LEVINE:

8 **Q.** And what happened to the phone after someone from CBP
9 brought it into the conference room?

11:07:01 10 **A.** They provided it to the computer forensics examiner
11 there in the room.

12 **Q.** And what did that forensic examiner do?

13 **A.** He made an image of the cellphone, which means he made
14 an exact copy on the computer of all the data that was
11:07:18 15 contained on the cellphone.

16 **Q.** And did you later review the data from the image made
17 of that phone?

18 **A.** Yes, I did.

19 **Q.** When did you begin your review of the data from the
11:07:27 20 image made of that phone?

21 **A.** The very next morning in the Miami FBI office.

22 **Q.** And was some of the data you reviewed the next morning
23 a log of Jabber chat conversations?

24 **A.** Yes, it was.

11:07:38 25 **Q.** At a general level, what is jabber?

Diaz - Direct/Levine

1 **A.** Jabber is an instant messaging system that is
2 encrypted so that only you and the person that you're
3 talking to can read the chat messages.

4 **Q.** Is Jabber chat always encrypted?

11:07:56 5 **A.** It's not always encrypted. It is an option that you
6 have to turn on to make the chats encrypted.

7 **Q.** Okay. And were the chat conversations that you
8 reviewed encrypted or not encrypted?

9 **A.** The ones we reviewed on the cellphone were unencrypted
11:08:18 10 chat conversations.

11 **Q.** And were the chat conversations you reviewed largely
12 in Romanian?

13 **A.** Yes, they were.

14 **Q.** Were you part of the team that surveilled Danet while
11:08:27 15 he was in the country?

16 **A.** Yes.

17 **Q.** Showing you what's been -- I'd like to bring up what's
18 been previously marked as Government's Exhibit 385. Just
19 for us here.

11:08:43 20 THE COURT: Well, it's the photo, folks. Any
21 objection?

22 MR. O'SHEA: No objection.

23 THE COURT: All right.

24 MR. LEVINE: We don't see it yet.

11:09:00 25 MS. CHANDLER: I haven't put it up. I don't

Diaz - Direct/Levine

1 think the Judge has turned over the jury.

2 MR. LEVINE: Oh. Your Honor, the jury screen
3 is apparently still on, your Honor.

4 THE COURT: Any objection, Mr. Goldberg?

11:09:11 5 MS. CHANDLER: They haven't seen it yet.

6 MR. O'SHEA: There it is. No objection,
7 Judge.

8 MR. GOLDBERG: No objection.

9 THE COURT: All right. It will be admitted.

11:09:23 10 MR. LEVINE: Okay. Permission to publish it
11 to the jury.

12 THE COURT: It's admitted. So, of course.

13 MR. LEVINE: Thank you.

14 Q. And what is Government's Exhibit 385?

11:09:31 15 A. This is a picture taken in the Miami International
16 Airport on May 14, 2015.

17 Q. Is Government's Exhibit 385 a fair and accurate
18 photograph of Danet at Miami International Airport?

19 A. Yes, it is.

11:09:46 20 Q. Looking at Government's Exhibit 385, could you please
21 circle Danet on your screen? Hopefully that will work.

22 A. It's not making any marks.

23 THE JURY: We can see it.

24 Q. Okay. Can you describe him in the photograph as well
11:10:02 25 just for the record?

Diaz - Direct/Levine

1 **A.** Yes.

2 So you can see his side view. He has black hair.

3 Looks like he's wearing jeans and maybe a gray shirt with a
4 black backpack, I think.

11:10:14 5 **Q.** Does he appear to be standing immediately behind or
6 next to the right of the person with the white hat?

7 **A.** Yes.

8 **Q.** All right.

9 Was May 14, 2015 the first time you saw Danet in
11:10:29 10 person?

11 **A.** Yes, it was.

12 **Q.** Had you seen photographs of Danet prior to him landing
13 in Miami?

14 **A.** Yes, I had.

11:10:35 15 **Q.** Where were those photos from?

16 **A.** He had previously received a visa to visit the United
17 States. And so there was a picture of him on the visa
18 paperwork, in the database.

19 **Q.** Okay. And had you seen any other pictures of Danet
11:10:55 20 from his passport?

21 **A.** From his passport, I think it's the same picture
22 that's on the visa.

23 **Q.** Okay.

24 And you said Danet had previously had been in the visa
11:11:05 25 database because we previously been to the United States?

Diaz - Direct/Levine

1 **A.** Yes.

2 **Q.** Do you know why that was?

3 **A.** In 2011, Tiberiu Danet was an intern at Google in
4 California.

11:11:20 5 **Q.** I'd like to show you what's been marked previously as
6 Government's Exhibit 1896.

7 MR. O'SHEA: One moment please, Judge.

8 THE JURY: We can see this.

9 MR. O'SHEA: I don't think the jury should see
11:11:42 10 it yet.

11 THE COURT: They're not.

12 MS. CHANDLER: Yes, they do.

13 MR. O'SHEA: Now, we can't see it.

14 MS. CHANDLER: I took it down because it was
11:11:52 15 going to the jury.

16 THE COURT: No, it's not going to the jury.

17 MR. O'SHEA: 1896.

18 BY MR. LEVINE:

19 **Q.** And what is Government's Exhibit 1896?

11:12:16 20 **A.** This is the -- well, the one that I -- the page I see
21 right now is the cover letter for the visa records for
22 Tiberiu Danet.

23 **Q.** Okay.

24 Is -- is Government's Exhibit 1896 a certified copy of
11:12:30 25 Danet's visa records?

Diaz - Direct/Levine

1 **A.** Yes, it is.

2 **Q.** And is Government's Exhibit 96, 1896 a fair and
3 accurate certified copy of Tiberiu Danet's visa records?

4 **A.** Yes, it is.

11:12:40 5 MR. LEVINE: Is there any --

6 MR. O'SHEA: Just -- I'm sorry, Judge. Let me
7 stand. Just a quick moment. The document itself is seven
8 pages long.

9 MR. LEVINE: Your Honor, this was subject to a
11:12:53 10 stipulation beforehand. It's a certified visa record.

11 MR. O'SHEA: That's not what we're talking
12 about, the authentication.

13 MS. CHANDLER: I can go through each page for
14 you.

11:13:13 15 MR. O'SHEA: Can I discuss something with
16 Brian in attempt to resolve this?

17 THE COURT: Sure.

18 (Counsel conferring.)

19 BY MR. LEVINE:

11:13:39 20 **Q.** All right.

21 So I believe you testified that this is a fair and
22 accurate certified copy of Danet's visa records?

23 **A.** Yes, it is.

24 **Q.** Okay. All right. So now I want to fast forward in
11:13:52 25 time.

Diaz - Direct/Levine

1 At some point, did a Grand Jury meet and indict Danet
2 and the two Defendants sitting here today?

3 **A.** Yes, they did.

4 **Q.** And we're going to hear from other Bayrob members
11:14:08 5 throughout this trial. Why weren't those other Bayrob
6 members indicted at the same time?

7 **A.** At the time, this was in July 2016, we only had enough
8 evidence to indict three of the Bayrob Group members that we
9 were aware of at the time.

11:14:27 10 **Q.** Okay.

11 So after the Grand Jury indicted Danet and these two
12 Defendants, did the United States make a request to the
13 Romanian Government to extradite these three?

14 **A.** Yes, we did.

11:14:41 15 **Q.** As part of the extradition request, what did the
16 United States have to do?

17 **A.** We had to provide information to the Romanian
18 authorities, detailing the charges for the Defendants, and
19 request to have them arrested in Romania and then have them
11:15:00 20 extradited back to the United States.

21 **Q.** And did the United States have to submit evidence or
22 does Romania just take the word from you?

23 **A.** Yes, we had to submit evidence to the Romanian
24 authorities, along with the charges.

11:15:13 25 **Q.** All right.

Diaz - Direct/Levine

1 And based on the information provided by the United
2 States, did Romania agree to extradite these three
3 individuals?

4 **A.** Yes, they did.

11:15:20 5 **Q.** Now did you travel to Romania to be involved in the
6 arrest of the Defendants and the seizure of their digital
7 devices?

8 **A.** Yes, I did.

9 **Q.** How many people from the FBI went to Romania to assist
11:15:33 10 with the arrest?

11 **A.** Six FBI employees traveled from the United States to
12 Romania, and then there were other FBI employees already in
13 Romania that assisted as well.

14 **Q.** Okay.

11:15:43 15 So who were the six that traveled to Romania to
16 assist?

17 **A.** So myself, Special Agent Ryan MacFarlane, and then
18 four computer forensics examiners, Peter Hammer, Yohel Diaz,
19 Dave Mingarelli, and Matt Frost.

11:15:59 20 **Q.** And a few days before the arrest, did you have
21 meetings in Romania to plan the take down?

22 **A.** Yes, we did.

23 **Q.** Okay. And did the meetings take place?

24 **A.** We initially had one meeting at the Romanian
11:16:14 25 Prosecutor's Office and then just before the take down, we

Diaz - Direct/Levine

1 had another meeting at the Romanian National Police
2 building.

3 Q. Okay.

4 And so we'll start with the meeting of the
11:16:24 5 Prosecutor's Office. What is the Prosecutor called in
6 Romanian?

7 A. It's DIICOT.

8 Q. Do you know what that stands for?

9 A. I believe Director of -- Directorate of Intelligence
11:16:36 10 and Terrorism. I'm not exactly sure.

11 Q. Okay.

12 But did they have a building in Romania?

13 A. Yes, they did do.

14 Q. Okay. Is that where you had this first meeting?

11:16:47 15 A. Yes.

16 Q. And who was physically present at the meeting that
17 you -- when you were figuring out the take down plan?

18 A. So the FBI team, the -- there were seven of us there;
19 the six that traveled over and then the ALLOT. There were a
11:17:02 20 couple of the Romanian Prosecutors there and there were
21 representatives for the Romanian National Police as well.

22 Q. I'd like to bring up for us only what has been marked
23 as Government's Exhibit Demonstrative 1845.

24 THE COURT: Well, if it's demonstrative, you
11:17:19 25 have every right to show it.

Diaz - Direct/Levine

1 MR. LEVINE: Okay.

2 Let's look at 1845.

3 Q. What is Government's Exhibit 1845, Special Agent Diaz?

4 A. It is a map of Romania.

11:17:30 5 Q. All right.

6 And does this map of Romania, Government's Exhibit
7 1845, fair and accurate depict the locations of the cities
8 where the take down was scheduled to take place?

9 A. Yes, it does.

11:17:40 10 Q. All right.

11 And would using this map of Romania help the jury
12 understand your testimony as to the locations of the cities
13 in Romania, where the take down was scheduled to take place?

14 A. Yes.

11:17:51 15 Q. Okay.

16 So looking at Exhibit 1845, what locations -- what was
17 law enforcement planning to visit on September 28, 2016?

18 A. Multiple locations in Bucharest and also one location
19 in Brasov.

11:18:09 20 Q. Okay.

21 So what -- so those are the cities. What actual
22 locations in those cities?

23 A. Okay.

24 So in Brasov, we were planning to do a search warrant,
11:18:22 25 and arrest Bogdan Nicolescu at his house in Brasov, Romania.

Diaz - Direct/Levine

1 And then in Bucharest, Romania, there was the apartment for
2 Tiberiu Danet as well as his arrest, the search warrant that
3 was conducted on an apartment for Bogdan Antonovich, and
4 then Radu Miclaus had multiple locations associated with
5 him. We did a search warrant at his father's house in
6 Bucharest, his girlfriend's apartment in Bucharest, an
7 apartment that he rented in Bucharest, and then there was
8 another location outside of the city that was in the country
9 that was associated with his grandmother.

11:18:46 10 Q. Okay. So let's -- let's go through this sort of one
11 at a time.

12 You mentioned Miclaus?

13 A. Yes.

14 Q. Him having a house. Where was that house located?

11:19:15 15 A. In Brasov, Romania.

16 Q. And can you just point on the -- on the monitor to
17 where that is? The record will reflect that the witness is
18 pointing to where it says B-R-A-S-O-V on the map of Romania?

19 MR. McDONOUGH: May we approach the witness,
11:19:35 20 your Honor, just to --

21 THE COURT: Sure.

22 Q. Thank you.

23 Now, the house in Brasov, who was believed to reside
24 in that house?

11:20:10 25 A. Bogdan Nicolescu resided in the house in Brasov.

Diaz - Direct/Levine

1 Q. And whose house was that rented under?

2 A. The house was actually rented under Radu Miclaus' name
3 but he no longer lived there.

4 Q. At one point, were they both living there?

11:20:26 5 A. Yes, they were.

6 Q. All right.

7 And then you mentioned another location. Was it the
8 location where Danet was, where was that?

9 A. Danet was located in Bucharest, Romania.

11:20:40 10 Q. Was that a house or apartment?

11 A. Apartment.

12 Q. All right.

13 And then you mentioned someone that I don't think
14 we've heard of yet. Antonovich was it?

11:20:49 15 A. Yes, that is correct. Bogdan Antonovich.

16 Q. Who is that?

17 A. He was another member of the Bayrob Group.

18 Q. What was -- what was his role believed to have been?

19 A. He was what we called a cash out guy. So his role was
11:21:01 20 simply the Bayrob Group members would have him arrange to
21 have money mules do pickups of wire transfers or have him
22 cash out funds in other ways.

23 Q. Okay. And where was his apartment located?

24 A. In Bucharest, Romania, as well.

11:21:22 25 Q. To be clear, if Antonovich had that involvement in the

Diaz - Direct/Levine

1 Bayrob Group, why wasn't he -- let me ask you, was he part
2 of the extradition request?

3 **A.** He was not.

4 **Q.** Why not?

11:21:37 5 **A.** Although we had information that made us believe that
6 he was a member of the Bayrob Group and what his function
7 was, we did not have enough evidence to indict him at that
8 time.

9 **Q.** Okay.

11:21:50 10 So then you mentioned a number of locations associated
11 with Miclaus, correct?

12 **A.** That is correct.

13 **Q.** Why -- how come you searched only one location for
14 each of these other people but so many different ones for
11:22:03 15 Miclaus?

16 **A.** So the other three people pretty much just had one
17 residence that they stayed in all the time, they lived in.
18 That was their apartment. That's where they were.

19 We understood that Radu Miclaus --

11:22:20 20 **MR. O'SHEA:** Objection.

21 **THE COURT:** Sustained.

22 **Q.** And just to clarify for the record, what is Radu
23 Miclaus' full name?

24 **A.** Radu Bogdan Miclaus.

11:22:29 25 **Q.** Okay. So you can continue.

Diaz - Direct/Levine

1 **A.** Radu Miclaus had multiple addresses --

2 MR. O'SHEA: Objection.

3 THE COURT: Overruled.

4 THE WITNESS: -- he was known to stay in.

11:22:41 5 MR. O'SHEA: Objection.

6 THE COURT: Well, sustained.

7 **Q.** Okay.

8 So were each of the locations that you searched for,
9 that were related to Miclaus, the locations --

11:22:56 10 MR. O'SHEA: Objection to the form of the
11 question.

12 MR. LEVINE: I haven't finished the question
13 yet.

14 THE COURT: No. Sustained.

11:23:02 15 **Q.** Were each of the locations that you searched that were
16 associated with Miclaus --

17 MR. O'SHEA: Objection.

18 MR. LEVINE: Strike that.

19 **Q.** Were each of the locations you searched related to
11:23:15 20 Miclaus ones that were associated with him?

21 MR. O'SHEA: Objection.

22 THE WITNESS: Yes.

23 THE COURT: Overruled. I'll allow that.

24 THE WITNESS: Yes, all of the locations were
11:23:25 25 associated with him.

Diaz - Direct/Levine

1 Q. Okay. All right.

2 So on the day of the actual arrest, what different
3 locations did each FBI person go to?

4 A. I went to, myself and others, went to the apartment
11:23:47 5 for Tiberiu Danet. Special Agent Ryan MacFarlane and a
6 computer forensics examiner, Matt Frost, went to Nicolescu's
7 house in Brasov. Forensic examiner Peter Hammer went to the
8 father of Radu Miclaus' house. And then the last computer
9 forensics examiner, Dave Mingarelli, went to Bogdan
11:24:11 10 Antonovich's apartment.

11 Q. Okay.

12 So at the time of the arrest, you went to Danet's
13 apartment in Bucharest?

14 A. That is correct.

11:24:20 15 Q. Who was with you when with you went to the amount
16 apartment in Bucharest; not just from the FBI but in who was
17 with you in total?

18 A. Computer Forensics Examiner Yohel Diaz. There was an
19 FBI employee that works there at the US Embassy. Her name
11:24:33 20 is Adina Barut. And then there was approximately, I
21 believe, five Romanian National Police officers with us.
22 And then in addition to that, they had the -- one of the
23 local Romanian SWAT teams enter the apartment before us.
24 And I believe there was four or five SWAT members there as
11:24:55 25 well.

Diaz - Direct/Levine

1 Q. All right.

2 And just to be clear, what is a SWAT member?

3 A. SWAT is -- I think we've all seen SWAT on TV. They're
4 usually police officers that enter into a location. For
11:25:08 5 whatever reason, is deemed maybe dangerous or another reason
6 why you need to do an immediate entry into that location.
7 And so they will go and they're usually, you know, usually
8 have on more protective clothing and, therefore, able to
9 better protect themselves in event of a dangerous encounter.

11:25:27 10 Q. In this particular situation, was the reason to use
11 SWAT that -- they thought it was a dangerous encounter or
12 something else?

13 A. It was something else. We --

14 MR. GOLDBERG: Objection.

11:25:39 15 THE COURT: Overruled.

16 THE WITNESS: We wanted to enter each location
17 dynamically, meaning that we wanted to not wait for the
18 person to come to the door and let us in. We wanted to
19 enter the location immediately in the hopes of the person in
11:25:55 20 the apartment or the house is on their computer and has
21 their computer open and unlocked. Therefore, allowing us to
22 do a better forensics examination of the computer.

23 Q. Well, what was the concern if the computer was not
24 open and unlocked?

11:26:12 25 A. We were concerned that all of the computers would be

Diaz - Direct/Levine

1 encrypted. And so if the individual either didn't provide
2 us the password or didn't have the computer open and
3 unlocked, then the computer itself would be encrypted and we
4 would not be able to do as good a forensics examination on
5 that computer.

11:26:30

6 Q. Because -- and is that because you wouldn't be able to
7 tell what was in the encrypted area?

8 A. Yes, that is correct.

9 Q. Now, how did you all get to Danet's apartment in
10 Bucharest?

11:26:43

11 A. We rode in a car with Adina Barut from the US Embassy.

12 Q. And I'm showing you what's been previously marked as
13 Government's Exhibit 1897, which is a photograph. So I
14 think we can show it to the jury. And what is Government's
15 Exhibit 1897?

11:27:09

16 A. This is a picture of the outside of the apartment
17 building for Tiberiu Danet.

18 Q. And who took these photographs?

19 A. I did.

20 Q. And did these photographs fairly and accurately depict
21 Danet's apartment building in Bucharest?

11:27:18

22 A. Yes, it does.

23 Q. All right.

24 MR. LEVINE: Your Honor, do I need to move to
25 admit this or do that later?

11:27:28

Diaz - Direct/Levine

1 THE COURT: Any objection?

2 MR. GOLDBERG: No objection.

3 THE COURT: Admitted.

4 Q. So what are we seeing here in the first photograph?

11:27:35 5 A. This is just the doorway to the apartment building,
6 the outside of the apartment building.

7 MR. LEVINE: Can we look at Page 2, please?

8 Q. And what are we seeing on the second photograph here?

9 A. The same doorway, just from, you know, further back.

11:27:50 10 Q. Okay. And could we look at the third photograph?

11 What are we seeing there?

12 A. That is the apartment building where Tiberiu Danet
13 lived.

14 Q. All right.

11:27:59 15 And is that also what we're seeing here on the fourth
16 photo?

17 A. Yes, it is.

18 Q. All right.

19 Who went into Danet's apartment first?

11:28:07 20 A. The Romanian SWAT team did.

21 Q. And where were you when the SWAT team went into
22 Danet's apartment?

23 A. I was standing in the hallway by the stairwell for the
24 apartment -- the apartment building.

11:28:21 25 Q. At some point, did you enter Danet's apartment?

Diaz - Direct/Levine

1 **A.** Yes, I did.

2 **Q.** When did you enter Danet's apartment?

3 **A.** After the SWAT team went in, they had made sure that
4 the apartment was safe for everyone else to enter. And so
11:28:34 5 the Romanian National Police went in and then myself and two
6 other FBI employees entered as well.

7 **Q.** And at that point, did you see Danet in his apartment?

8 **A.** Yes, I did.

9 **Q.** And did you recognize Danet from Miami and from his
11:28:53 10 pictures?

11 **A.** Yes, I did.

12 **Q.** While you were in Danet's apartment, did the Romanian
13 National Police find and seize any digital devices?

14 **A.** Yes, they did.

11:29:04 15 **Q.** What devices did the Romanian National Police find and
16 seize from Danet's apartment?

17 **A.** They seized multiple computers, a computer tower, some
18 laptops, a couple of cellphones, thumb drives, a couple
19 pieces of paper and some money.

11:29:20 20 **Q.** Okay.

21 Was one of the things that they seized from Danet's
22 apartment a Dell laptop?

23 **A.** Yes, it was.

24 **Q.** And was one of the things they seized from the
11:29:30 25 apartment a Miami phone?

Diaz - Direct/Levine

1 **A.** Yes.

2 **Q.** Was wan of the items a western digital hard drive?

3 **A.** Yes.

4 **Q.** All right.

11:29:37 5 What did the RNP do with the digital devices?

6 **A.** They would put them into the bags and seal them.

7 After -- first, they would make an inventory of everything

8 that they were taking. They would go through the inventory

9 with Tiberiu Danet. He would sign the inventory, agreeing

11:29:56 10 that that was all of the items that were seized, and then

11 they would place them all into bags and seal them.

12 **Q.** Okay.

13 When you say seal them, what do you mean?

14 **A.** They would actually take a piece of cardboard and use

11:30:09 15 like an old wax seal on the cardboard to seal it.

16 **Q.** Okay. Okay.

17 And I'm going to show you what's been previously

18 marked as Government's Exhibit 2429. What is Government's

19 Exhibit 2429?

11:30:45 20 **A.** These are multiple seals from multiple bags that they

21 had seized during the search warrants. Each one has a wax

22 seal on it, and then it also has the name of the subject at

23 that particular location with the address as well, and then

24 at least one signature of a Romanian National Police

11:31:07 25 officer.

Diaz - Direct/Levine

1 MR. LEVINE: Your Honor, I'd like to move the
2 admission of Government's Exhibit 2449.

3 MR. GOLDBERG: No objection.

4 MR. O'SHEA: No objection.

11:31:14 5 THE COURT: Admitted.

6 MR. LEVINE: Your Honor, what would be the
7 best way to show these to the jury? Pass them out?

8 THE COURT: The witness can hold it up,
9 perhaps.

11:31:23 10 MR. LEVINE: Can we turn on the Elmo and
11 maybe -- please hold it up but if --

12 THE COURT: You tell me what you want.

13 MR. LEVINE: Okay.

14 Can we pass it around to the jury?

11:31:42 15 THE COURT: Fine.

16 MR. LEVINE: All right.

17 **Q.** While they're passing those around, did you personally
18 watch the Romanian National Police put these seals on the
19 wax bags?

11:32:10 20 **A.** Yes, I did.

21 **Q.** How did they do that? Do they light a candle or
22 something?

23 **A.** I don't remember if they had to, if they had to heat
24 it up, but they -- they each have one that's assigned to
11:32:24 25 them. And so whenever they're going to do a search warrant,

Diaz - Direct/Levine

1 they make sure that they have their wax seal. And so they
2 would, you know, use the wax. I think they warmed it up
3 with a lighter, but I can't remember for sure, and then
4 stamp the cardboard.

11:32:42

5 Q. Okay.

6 I'd like to bring up -- well, let me -- I'm just going
7 to wait for it to go around to the jury, if that's okay,
8 your Honor.

9 And what were these wax seals placed on?

11:33:15

10 A. As you can see, it was on a piece of cardboard that
11 was attached to the bag that was containing the evidence
12 that was seized.

13 Q. And it appears to be string --

14 A. Yes.

11:33:26

15 Q. -- there as well. What is the string?

16 A. The string would tie the bag closed, and then hold the
17 cardboard to the bag.

18 Q. Okay.

19 And approximately how many bags did you see sealed
20 from Danet? Are we talking -- one bag or multiple bags?

11:33:49

21 A. Just from Danet's apartment?

22 Q. Just from Danet's apartment.

23 A. I think approximately maybe five.

24 Q. Okay.

11:33:59

25 But the exhibit contains examples of seals from all

Diaz - Direct/Levine

1 the different locations?

2 **A.** Yes, that is correct.

3 **Q.** Now, I'd like to bring up, just for us, Government's
4 Exhibit 402. Okay. And what is Government's Exhibit 402?

11:34:42 5 **A.** This is what's called a Proces-Verbal in Romania.

6 It is the document that they produce when they are
7 conducting a search warrant. And so this one is in regards
8 to the apartment for Tiberiu Danet for the search warrant on
9 his apartment.

11:35:02 10 **Q.** And did you see the Romanian National Police and Danet
11 filling out this form together?

12 **A.** Yes, I did.

13 **Q.** Okay. What do you recall about that interaction?

14 **A.** So the Romanian National Police would fill out the
11:35:15 15 form sitting right next to Tiberiu Danet. He could watch
16 them as they fill out the form. And they would, you know,
17 put his address, his information in there and list all of
18 the items that they were seizing and Tiberiu Danet reviewed
19 all those items that were on the form, and the actual
11:35:35 20 physical items there in the room.

21 **Q.** And were they speaking in Romanian or English?

22 **A.** Speaking in Romanian.

23 **Q.** Could you tell what they were saying?

24 **A.** Not very -- I couldn't tell myself very well. But, I
11:35:49 25 did have Adina Barut, who is the employee that works for the

Diaz - Direct/Levine

1 FBI at the US Embassy, and she was translating for me.

2 Q. And how would you describe the tone of the Romanian
3 National Police during this interaction?

4 A. They're very professional, very friendly.

11:36:05 5 Q. So there was no yelling?

6 A. No.

7 Q. No threats?

8 A. No.

9 Q. Did you hear or see any threats or coercion of any
11:36:12 10 kind?

11 A. No, no. In fact, the individual has the opportunity
12 at the beginning of the search warrant to request to have a
13 lawyer or a family friend present with them during the
14 search warrant.

11:36:26 15 Q. Okay. And did Danet request that?

16 A. He attempted to. He tried to call a lawyer. He tried
17 to call a couple of friends. But, he was not able to get a
18 hold of anyone to come over. It was early in the morning.

19 Q. Okay.

11:36:39 20 So where did you go after Danet was arrested, and the
21 RNP had seized Danet's digital devices?

22 A. Well, once we finished the apartment, we searched his
23 car.

24 Q. Okay.

11:36:55 25 A. So we did the search warrant of the car as well in the

Diaz - Direct/Levine

1 parking lot of the apartment.

2 Q. Where did you go after that?

3 A. After the search warrant of the car was complete, we
4 went to, back to the Romanian Prosecutor's Office, DIICOT.

11:37:08 5 Q. And what happened at the Romanian Prosecutor's Office?

6 A. Myself and Special Agent Ryan MacFarlane, we were able
7 to sit in on interviews that were being conducted by the
8 Romanian Prosecutor with the -- with the Defendants as well
9 as other members of the Bayrob Group and some other
10 witnesses that were being interviewed.

11 Q. So specifically, whose interviews did you sit in on?

12 A. I sat in on the interview of Roger Miclaus, Radu
13 Miclaus, Tiberiu Danet, Tiberiu Danet's brother, and Bogdan
14 Antonovich, his brother, and his wife, and Miclaus'
11:37:51 15 girlfriend, and Radu Miclaus' ex-girlfriend.

16 Q. And just to be clear, other than the three --
17 Nicolescu, Danet, and Miclaus -- were any of the other
18 people under arrest?

19 A. No, they were not.

11:38:07 20 Q. And why weren't they under arrest at that time?

21 A. We did not have evidence -- enough evidence to charge
22 any of them at that time.

23 Q. Okay.

24 Now, do you recognize any of the people you just
11:38:19 25 mentioned in the courtroom today?

Diaz - Direct/Levine

1 **A.** I do. Can I correct one mistake that I --

2 **Q.** Of course.

3 **A.** Sorry.

4 Tiberiu Danet's brother was not interviewed. I was
11:38:31 5 mistaking him with Antonovich's brother. So we did not
6 interview Tiberiu Danet's brother at that time.

7 **Q.** Okay.

8 To be clear, with respect to the full list of people
9 that were interviewed, were there some people who weren't
11:38:44 10 even suspected to be part of the Bayrob Group?

11 **A.** Yes, that is true.

12 **Q.** So why were those people interviewed?

13 **A.** We were interviewing them to see if they could provide
14 information about the Bayrob Group member that they -- that
11:38:58 15 they knew.

16 **Q.** Okay.

17 And of the people that you saw, you sat in on
18 interviews, do you recognize any of those people sitting in
19 the courtroom today?

11:39:09 20 **A.** Yes, I do.

21 **Q.** Who do you recognize in the courtroom today?

22 **A.** I recognize Bogdan Nicolescu and Radu Miclaus.

23 **Q.** Could you please identify them for the record, if you
24 would first identify Bogdan Nicolescu for the record?

11:39:20 25 **A.** Bogdan Nicolescu is sitting at the table next to his

Diaz - Direct/Levine

1 attorney, wearing a black suit jacket and a blue shirt.

2 And then Radu Miclaus is at the end of the table
3 wearing, I think, a blue suit jacket and a blue shirt.

4 MR. LEVINE: Okay. Thank you.

11:39:38 5 Q. Now do you recall meeting at the Romanian Prosecutor's
6 Office again on October 1, 2016?

7 A. Yes, I do.

8 Q. And what happened during that meeting?

9 A. That is when the Romanian Prosecutor, the Romanian
11:39:54 10 authorities provided all of the evidence that was collected
11 throughout all of the search warrants to myself.

12 Q. Okay. And who was present there?

13 A. So there was from the FBI myself, three of the
14 computer forensics examiners, Diaz, Peter Hammer, and Dave
11:40:15 15 Mingarelli, and then a couple of Romanian National Police
16 officers were there, I think two or three, and then the
17 Romanian Prosecutor was there as well.

18 Q. Okay. I'm sorry.

19 MR. LEVINE: I have to go back for a second
11:40:28 20 and just say may the record reflect that this witness has
21 identified the Defendants?

22 THE COURT: Ma'am, do they have ties on or
23 not?

24 THE WITNESS: No, neither one of them have on
11:40:37 25 ties.

Diaz - Direct/Levine

1 THE COURT: The record may so reflect.

2 MR. LEVINE: Thank you, your Honor.

3 Q. Okay.

4 So when you got to the Romanian Prosecutor's Office,
11:40:53 5 were the digital devices, where were the digital devices?
6 Were they just out?

7 A. They were still contained in the bags that they had
8 been wrapped up in during the search warrants. They were in
9 the Prosecutor's Office.

11:41:04 10 Q. So how many bags was that?

11 A. I believe approximately 20 to 25, maybe.

12 Q. Okay. And were the wax seals still on the bags?

13 A. Yes, they were.

14 Q. I'd like to show just the witness what has previously
11:41:21 15 been marked as Government's Exhibit 4, which is an 11-page
16 exhibit, plus an English translation. Okay.

17 Is -- what is Government's Exhibit 4?

18 A. This is another Proces-Verbal is what it's called in
19 Romania, and it is a document that lists out every single
11:41:44 20 item of evidence that was seized during all of the different
21 search warrants.

22 Q. Okay. And did you sign this?

23 A. Yes, I did.

24 Q. Is it a fair and accurate copy of the inventory list
11:41:57 25 that you signed?

Diaz - Direct/Levine

1 **A.** Yes, it is.

2 **Q.** And who else -- who else signed this exhibit?

3 **A.** The Romanian Prosecutor, Silvia Popa, and then two
4 Romanian police officers, Vasile Belciu, I'm sure if I'm
11:42:14 5 pronouncing that right, and Ramona Musat.

6 **Q.** Did all four of you sign every page of this exhibit?

7 **A.** Yes, we did.

8 **Q.** Okay.

9 Does this inventory list all the devices that were
11:42:25 10 seized from Romania, along with the location of the seizure
11 and the person seized from?

12 **A.** Yes, it does.

13 **Q.** At some point, did you compare what was on the
14 inventory list to what was in the bags to make sure
11:42:37 15 everything was accounted for?

16 **A.** Yes. There in the Romania Prosecutor's Office, I went
17 through the inventory list and made sure that every single
18 bag listed on the inventory list was there and accounted
19 for.

11:42:50 20 **Q.** Okay.

21 But my question was at some point, did you compare
22 what was on the inventory list to what was in the bags to
23 make sure everything was accounted for?

24 **A.** Yes, I'm sorry.

11:43:01 25 Once the items were shipped to the Cleveland FBI

Diaz - Direct/Levine

1 office, that's when I opened every single bag and compared
2 the contents of the bags to the inventory list.

3 Q. And did they match?

4 A. Yes, they did.

11:43:14 5 Q. Okay.

6 So going back, where did you bring the bags with the
7 digital devices?

8 A. So when I took control of them, took possession of
9 them at the Romanian Prosecutor's Office, we -- I initially
11:43:28 10 first took them to the hotel that we were staying at in
11 Bucharest, Romania.

12 Q. Did the FBI image any of the digital devices right
13 there in the hotel?

14 A. Yes.

11:43:38 15 Q. Which devices were imaged in the hotel?

16 A. We imaged items that were -- that belonged to Bogdan
17 Antonovich and items that belonged to the girlfriend of Radu
18 Miclaus and the grandmother of Radu Miclaus.

19 Q. Why were those items imaged right away?

11:43:58 20 A. We wanted to be able to return those item. We did
21 not -- well did not expect to find as much evidence on those
22 items and, therefore, we were going to return those items to
23 their owners immediately.

24 Q. And were those owners of items, were those owners
11:44:18 25 under arrest?

Diaz - Direct/Levine

1 **A.** No, they were not.

2 **Q.** Okay.

3 Who imaged Antonovich's devices?

11:44:30

4 **A.** I'm not sure between the different cart examiners who
5 imaged which items.

6 **Q.** But it was one of the three cart examiners?

7 **A.** Yes.

8 **Q.** Again what does it mean to image a device?

11:44:40

9 **A.** It is to make an exact copy of all of the data files
10 and all the information contained on that device and copy it
11 onto a computer.

12 **Q.** Okay.

13 And then what happened to Defendants' digital devices
14 from there?

11:44:50

15 **A.** So I actually provided all of them to the ALATT, Peter
16 Trayvan in Bucharest, Romania.

17 **Q.** And he works out of the embassy?

18 **A.** Yes, he does.

19 **Q.** What was he supposed to do with them?

11:45:05

20 **A.** The ones that were being returned, he made contact
21 with those individuals and made arrangements to return their
22 items to them. And all of the rest of them, he FedExed to
23 the FBI office in Cleveland.

24 **Q.** All right.

11:45:19

25 And did those digital devices arrive in the US via

Diaz - Direct/Levine

1 Fed-Ex?

2 **A.** Yes, they did.

3 **Q.** And once they arrived, did you open them and go
4 through the items in the bags to make sure that everything
11:45:29 5 on the inventory, Government's Exhibit 4, was present?

6 **A.** Yes, I did.

7 **Q.** And was everything present and accounted for?

8 **A.** Yes, it was.

9 **Q.** Where were the digital devices stored once they
11:45:40 10 arrived in the U.S. via Fed-Ex?

11 **A.** In the FBI evidence control room.

12 **Q.** Okay.

13 And were these digital devices, the ones that hadn't
14 been imaged before, were they later imaged?

11:45:53 15 **A.** Yes, they were.

16 **Q.** And where were they imaged?

17 **A.** In multiple FBI offices. Many of them were imaged
18 here in Cleveland, but we also sent some of them to
19 headquarters in Washington, D.C., and some of them went to
11:46:07 20 another office out in Pocatello.

21 **Q.** I'm showing you what has been marked as Government's
22 Exhibit 2008. What is Government's Exhibit 2008?

23 **A.** This is a laptop that belonged to Tiberiu Danet.

24 **Q.** Okay. And where was this laptop seized from?

11:46:37 25 **MR. O'SHEA:** Objection. Can we just approach

Diaz - Direct/Levine

1 very quickly on this, your Honor? Very quickly.

2 THE COURT: Okay.

3 (The following proceedings were held at side bar:)

4 MR. O'SHEA: Here's the basis of my objection.

11:47:04 5 The -- this witness has not gone into any foundation
6 identifying who owned what computer. That's all presumed by
7 the Government. I'm not conceding that.

8 There's -- for instance, there's stuff on these
9 Romanian search warrants, if we want to call them that, that
11:47:21 10 this is theirs and we are not conceding that our clients
11 owned or possessed these items. We're not.

12 So the question of the witness presumes that this is
13 Danet's stuff, this is Radu Miclaus' stuff.

14 THE COURT: Well, it can be identified as
11:47:42 15 something that was taken from a particular place, and if
16 it's Danet's place, then that -- then that has to be
17 identified as something from taken from his place, not
18 necessarily Danet's. The jurors can certainly make any
19 conclusion they want.

11:48:01 20 MR. O'SHEA: Absolutely.

21 MR. LEVINE: No objection.

22 (Proceedings resumed within the hearing of the jury:)

23 BY MR. LEVINE:

24 Q. So is Government's Exhibit 2008 a Dell laptop seized
11:48:24 25 from Danet's apartment?

Diaz - Direct/Levine

1 **A.** Yes, it is.

2 **Q.** And how can you tell that Government's Exhibit 2008 is
3 a Dell laptop seized from his apartment?

4 **A.** The primary way is by comparing the serial number on
11:48:38 5 the laptop to the evidence inventory list. I also color
6 coded all of them. So I know immediately by looking at it
7 that it belonged -- that it was in Tiberiu Danet's
8 apartment.

9 **Q.** And did you compare the laptop serial number to the
11:48:56 10 serial number on the inventory list before taking the stand
11 today?

12 **A.** Yes, I did.

13 **Q.** Okay.

14 MR. LEVINE: I move to admit Government's
11:49:05 15 Exhibit 2008.

16 MR. GOLDBERG: No objection.

17 MR. O'SHEA: No objection.

18 THE COURT: Admitted.

19 MR. LEVINE: Okay.

11:49:09 20 **Q.** I am showing you what's been previously marked inside
21 this envelope as Exhibit 399.

22 Is Government's Exhibit 399 -- I don't know if I'm
23 pronouncing this right -- a Xiaomi phone seized from Danet's
24 apartment?

11:49:42 25 **A.** Yes, it is.

Diaz - Direct/Levine

1 Q. And how can you tell that Government's Exhibit 399 is
2 a phone seized from Danet's apartment?

3 A. By comparing the serial number that's inside the phone
4 with the inventory list.

11:49:53 5 Q. Okay.

6 Can you hold up the phone so that the jury can see?

7 All right. Thank you.

8 MR. LEVINE: I move to admit Government's
9 Exhibit 399.

11:50:01 10 MR. GOLDBERG: No objection.

11 MR. O'SHEA: No objection.

12 THE COURT: I'm sorry, Mr. O'Shea?

13 MR. O'SHEA: Sorry, Judge. No objection.

14 THE COURT: Admitted.

11:50:08 15 Q. Now handing the witness what has previously been
16 marked as Government's Exhibit 2274, 2274, is Government's
17 Exhibit 2274 a hard drive seized from Danet's apartment?

18 A. Yes, it is.

19 Q. And how can you tell that Government's Exhibit 2274 is
11:50:43 20 a hard drive seized from Danet's apartment?

21 A. Again, by comparing the serial number on the back of
22 the hard drive with the items that are on evidence inventory
23 list.

24 Q. Okay.

11:50:55 25 MR. LEVINE: Move to admit Government's

Diaz - Direct/Levine

1 Exhibit 2274.

2 MR. GOLDBERG: No objection, Judge.

3 MR. O'SHEA: No objection, Judge.

4 THE COURT: Admitted.

11:51:00 5 BY MR. LEVINE:

6 Q. Okay.

7 Have you reviewed the other digital devices on the
8 evidence listed in the courtroom today to confirm they're
9 the same items seized during the arrest of the Bayrob Group?

11:51:11 10 A. Yes, I have.

11 Q. And how were you able -- were you -- were they the
12 same items?

13 A. Yes, they were.

14 Q. And how were you able to tell that it was the same
11:51:18 15 items seized during the arrest of the Bayrob Group?

16 MR. O'SHEA: Objection.

17 THE COURT: Overruled.

18 THE WITNESS: Most of them have a serial

19 number that I can compare with the serial number on the
11:51:28 20 evidence inventory list. If it is an item such as a thumb
21 drive, it doesn't necessarily have a serial number, but the
22 Romanians wrote down descriptions of what they look like or
23 the name of the type of thumb drive on the evidence
24 inventory list.

11:51:43 25 Q. So okay.

Diaz - Direct/Levine

1 And could you also -- were you also the one who
2 removed the wax seals from these items?

3 **A.** Yes.

4 **Q.** And you recognized them from when you saw them -- when
5 you opened the wax seals?

6 **A.** Yes, I recognize the ones from Tiberiu Danet's
7 apartment, but also on the inventory list, the way that the
8 Romanian National Police had inventoried everything on the
9 list, they actually wrote what was in each specific bag. It
10 was broken out by bag. So that was helpful for me when
11 removing all of the contents from the bag.

12 If there was a thumb drive in there, I could look for
13 the description in that particular bag for the thumb drive.

14 (Counsel conferring.)

15 **MR. LEVINE:** No further questions for this
16 witness, your Honor.

17 **THE COURT:** Ladies and gentlemen, I think this
18 is a good place to take a break.

19 Please remember the admonition. Do not form any
20 opinion and do not talk about the case.

21 Please be downstairs at 1:00. We will call for you at
22 that time and bring you up. Have a good lunch, everybody.

23 All rise for the jury.

24 (Thereupon, a luncheon recess was had.)

13:06:22 25

Diaz - Cross/Goldberg

1 TUESDAY SESSION, MARCH 26, 2019, AT 1:06 P.M.

2 THE COURT: Cross-examination, Mr. Goldberg.

3 MR. GOLDBERG: Thank you, your Honor.

4 CROSS-EXAMINATION OF STACY DIAZ

13:10:15 5 BY MR. GOLDBERG:

6 Q. Good afternoon, Special Agent. A couple questions.

7 You mentioned that the Romanian office of the FBI
8 that's in the -- in the embassy went from one full-time
9 agent to six full times agents?

13:10:29 10 A. Yes, that's correct.

11 Q. How long has it been six full-time agents?

12 A. I don't know exactly. I would say approximately maybe
13 the last four years.

14 Q. Okay.

13:10:39 15 Safe to assume that fraud, Internet fraud, malware
16 issues continue to occur in the state of Romania?

17 A. Yes, in the country of remain.

18 Q. And that is the basic focus of the FBI having those
19 six agents in Romania?

13:11:01 20 A. That is one of their focuses, yes.

21 Q. So not only did the general problem of fraud over the
22 Internet continue after the arrest of the Defendants in this
23 case, but it has in fact increased and has required more and
24 more manpower for the United States to address?

13:11:32 25 A. I don't know the specific statistics, yes, I mean we

Diaz - Cross/Goldberg

1 had six FBI agents working there before the arrest of the
2 Defendants and we continue to have six FBI agents.

3 **Q.** I understand your testimony that once the Defendants
4 were arrested, the conspiracy that you identified as Bayrob
13:11:53 5 stopped operating?

6 **A.** That is correct.

7 **MR. LEVINE:** Objection, your Honor.

8 **THE COURT:** Overruled.

9 **BY MR. GOLDBERG:**

13:12:02 10 **Q.** And that's not unusual when persons get arrested that
11 other persons who may or may not be -- or may be involved in
12 a conspiracy would cease their involvement with that
13 conspiracy because of the compromise that the arrest has
14 caused?

13:12:22 15 **A.** I'm not sure I understand.

16 **Q.** So you arrest somebody, and obviously there's many
17 other people that are involved in the Bayrob conspiracy?

18 **A.** Yes.

19 **Q.** Correct? And you made arrests of certain individuals.
13:12:35 20 It wouldn't be unusual for all the activity involving
21 everybody in that particular group to cease. That wouldn't
22 be unusual, would it?

23 **A.** No, I guess not.

24 **Q.** No, because whether it's somebody who is low down or
13:12:55 25 high up or peripherally involved, it creates a risk for the

Diaz - Cross/Goldberg

1 other members to be continuing with their activity?

2 **A.** Yes.

3 **Q.** Okay.

4 So earlier in your testimony, you talked about IP
13:13:09 5 addresses and how they change automatically?

6 **A.** Yes.

7 **Q.** So if one has a static IP address, does that mean it
8 stays the same all the time or that it still be changed
9 every once in a while?

13:13:24 10 **A.** If you have a static IP address, it's going to stay
11 the same generally. There may be instances in which it
12 changes, but for the most part, it's going to stay.

13 **Q.** And the dynamic IP address is one that changes?

14 **A.** More often, yes.

13:13:39 15 **Q.** And a dynamic IP address can change everyday or every
16 week, month?

17 **A.** It varies, yes.

18 **Q.** There's no limit on that parameter, it can change at
19 any time?

13:13:52 20 **A.** That is correct.

21 **Q.** Nothing illegal about doing that, correct?

22 **A.** No, there's nothing illegal about changing your IP
23 address.

24 **Q.** In and of itself?

13:13:58 25 **A.** Correct.

Diaz - Cross/Goldberg

1 Q. All right.

2 So I understand that you early on were corresponding
3 with the Romanian National Police regarding the M-LAT
4 request?

13:14:09 5 A. Yes.

6 Q. Am I correct in stating that over the course of your
7 early investigation, say from 2009 to 2013, that you
8 requested and received information pursuant to the M-LAT
9 request 50 times from the Romanian National Police?

13:14:32 10 A. No, actually, I believe the first actual M-LAT was
11 later in the investigation, early on it was just -- I was
12 sending information to the LEGATT office in Romania and they
13 were just requesting simple database checks from the
14 Romanian National Police.

13:14:49 15 Q. When you got -- when it got into the warrants for
16 certain or search warrants or communications intercepts,
17 then you actually made M-LAT requests?

18 A. That's correct.

19 Q. And the Romanian National Police cooperated with you
13:15:07 20 in that regard?

21 A. Yes, the Romania authorities, the police, the
22 Prosecutor's Office.

23 Q. And whatever process they had to go through in Romania
24 wasn't your concern, it was their concern?

13:15:22 25 A. That is correct.

Diaz - Cross/Goldberg

1 Q. All right.

2 Did you ever ask them for anything and they said oh,
3 no, we can't do that?

4 A. There would be times that they would tell us, yes,
13:15:32 5 that there were certain things that were not allowed in
6 their legal system.

7 Q. Okay.

8 What about if -- let's say the FBI copied a house key,
9 and could that be used to execute a warrant in Romania?

13:15:51 10 A. It's my understanding from Romanian law, which I'm not
11 an expert on, but my understanding is yes, that could be
12 used.

13 Q. So that's what happened with Mr. Danet, correct?

14 A. That is correct.

13:16:03 15 Q. So in addition to all of these electronic devices we
16 heard about here today, one thing we didn't hear about was
17 the fact that Mr. Danet also had his house key taken from
18 him at the Miami National Airport?

19 A. It was copied, yes.

13:16:18 20 Q. Well, I mean it was taken as part of the search?

21 A. Yes.

22 Q. And it was copied?

23 A. And then given back to him.

24 Q. Given back to him?

13:16:26 25 A. Yes.

Diaz - Cross/Goldberg

1 Q. And then the copy of the key was somehow sent to the
2 Romanian National Police to use in their investigation?

3 A. That is correct.

4 Q. And part of that investigation was to enter into
13:16:40 5 Mr. Danet's apartment and to place listening devices so that
6 the Romanian National Police could watch him or listen to
7 him during the course of this investigation?

8 A. That is correct.

9 Q. And video devices as well?

13:16:52 10 A. They did not place video. They were not able to.

11 Q. Do you know whether the FBI has equipment that would
12 allow it to determine whether a particular person or a
13 particular person in a particular residence was actively on
14 the Internet at that moment?

13:17:18 15 A. Like a digital device that you would put on a computer
16 to determine who is --

17 Q. Yeah?

18 A. No, I mean I think that for the most part, we would
19 use multiple devices, a video camera to determine who was at
13:17:33 20 the keyboard.

21 Q. Okay.

22 So if you -- you have the power as an FBI agent and
23 the authority to ask the Romanian National Police to place
24 listening and video equipment in the Defendant's homes prior
13:17:55 25 to the searches, correct?

Diaz - Cross/Goldberg

1 **A.** The US Government does, yes.

2 **Q.** Okay. Well --

3 **A.** Yeah.

13:18:06

4 **Q.** And that was not something that was undertaken as part
5 of the search and arrest of the Defendants in this case?

6 **A.** No, it was prior to the search and arrest.

13:18:26

7 **Q.** So if that had been done, perhaps the FBI -- the
8 Romanian National Police and FBI wouldn't have had to guess
9 whether or not a particular Defendant was on his computer
10 when they entered?

11 MR. LEVINE: Objection.

12 THE COURT: Sustained.

13:18:43

13 **Q.** Well, you indicated that it is an investigatory
14 benefit to the FBI or the investigators if the subject is
15 actively on their computer when you enter?

16 MR. LEVINE: Objection.

17 THE COURT: Well, is that true, ma'am? Did
18 you indicate that?

13:18:54

19 THE WITNESS: I think I said that earlier
20 today.

21 **Q.** Right. Okay.

22 And what steps, if any, were taken to try to secure
23 that circumstance when you -- when these warrants were
24 executed?

13:19:10

25 **A.** So when we did the take down, we took steps to have

Diaz - Cross/Goldberg

1 someone online communicating with a Bayrob Group member. So
2 we were trying to determine -- to ensure that one of them
3 would be actively on their computer with it unlocked and
4 usable when we did the take down.

13:19:34 5 **Q.** And did that occur with regard to any of the
6 Defendants in this case?

7 **A.** No, none of them were on their computer when we
8 conducted the search warrant.

9 **Q.** But, there was -- somebody was on a computer somewhere
13:19:47 10 that you considered to be part of the Bayrob Group?

11 **A.** That is correct.

12 **Q.** All right.

13 You talked about 19,000 e-mails that were in the Read
14 Notify server. Correct me if I'm -- if I misstated --

13:20:06 15 **A.** They at one point were sent by the Read Notify server.
16 They were not saved on the server.

17 **Q.** Okay.

18 And those were provided to you pursuant to the
19 warrants?

13:20:17 20 **A.** No, they were not.

21 **Q.** They were provided by the Read Notify company itself?

22 **A.** That's correct. The company was determined to be a
23 victim in the case.

24 **Q.** Okay.

13:20:26 25 And so they collected these -- these e-mails and

Diaz - Cross/Goldberg

1 provided them to you?

2 **A.** Yes.

3 **Q.** And did you personally look at all 19,000 or did you
4 gather the relevant e-mails from some type of electronic
5 search?

13:20:46

6 **A.** I had a team at the FBI. Obviously there's no way I
7 could personally look at 19,000 e-mails. I personally
8 looked at over a couple -- over 2000 e-mails.

9 There was a team of, I believe, approximately eight or
10 nine FBI employees, and we divvied up the 19,000 e-mails
11 amongst us and we personally manually went through and
12 looked at every single e-mail.

13:21:03

13 **Q.** Okay.

14 And were there duplicates in those 19,000?

13:21:19

15 **A.** Duplicate e-mails?

16 **Q.** Yeah.

17 **A.** There may have been. I don't remember any.

18 **Q.** You can't testify that there were 19,000 distinct
19 e-mails. There may have been duplicates, correct?

13:21:31

20 **A.** There may have been duplicates.

21 **Q.** And you can't testify that every e-mail that is -- was
22 sent by a member of the alleged Bayrob conspiracy was read,
23 only the ones that were responded to?

24 **A.** Oh, read by the intended recipient?

13:21:50

25 **Q.** Yeah.

Diaz - Cross/Goldberg

1 **A.** No, I cannot say that it was definitely read.

2 **Q.** Only when there was some kind of response do you know
3 that it was read?

4 **A.** I do know that it was read, yes.

13:22:00 5 **Q.** You talked about Western Union and trying to catch --
6 or apprehend or observe the money mules picking up money.

7 **A.** Yes.

8 **Q.** Western Union -- would you say they were cooperative
9 with the investigation?

13:22:27 10 **A.** Yes.

11 **Q.** I mean if they were cooperative, what did they do to
12 try to help you locate or observe the actual pick up of
13 these monies in Europe?

14 **A.** They didn't do anything more than respond to the legal
13:22:45 15 process that I provided. I mean they would provide a spread
16 sheet, detailing all of the details for each transaction. I
17 would request them, I would give them names and countries of
18 transfers that I was interested in. They would search their
19 database and provide back all transactions for those
13:23:06 20 particular names in those particular countries.

21 **Q.** Was this historical, though?

22 **A.** Yes.

23 **Q.** Did you have any real time information that you could
24 have given to Western Union about a transaction that was in
13:23:19 25 progress?

Diaz - Cross/Goldberg

1 **A.** No.

2 **Q.** When Mr. Danet arrived in Miami, was he traveling
3 alone?

4 **A.** No, he was not.

13:23:38 5 **Q.** Who was he with?

6 **A.** Alexander Marin.

7 **Q.** Are you aware when he left the United States on that
8 trip?

9 **A.** Yes, it was in June of 2015. I don't remember the
13:23:54 10 exact date, early June.

11 **Q.** Did he travel to the US with the same companion?

12 **A.** Yes, he did.

13 **Q.** Was that person's electronic devices seized and
14 copied?

13:24:05 15 **A.** No, it was not.

16 **Q.** And that person who Mr. Danet was with was not on your
17 radar?

18 **A.** No, he was not.

19 **Q.** And you would agree that as far as you know, Mr. Danet
13:24:21 20 had -- well here. Strike that.

21 You indicated that the home in Brasov, is that how you
22 pronounce it?

23 **A.** Brasov.

24 **Q.** Brasov?

13:24:37 25 **A.** Um-hum.

Diaz - Cross/Goldberg

1 Q. You're attributing to Mr. Nicolescu as his residence
2 was rented originally by Mr. Miclaus?

3 A. That's correct.

4 Q. And it's -- Mr. Miclaus rented that home in 2009,
13:24:53 5 roughly?

6 A. I don't know the exact time.

7 Q. Was it years? He lived there for years?

8 A. It's my understanding he lived there for a couple
9 years.

13:25:00 10 Q. Okay.

11 Well, is it your understanding that there was items of
12 personal property in that home that belonged to Mr. Miclaus
13 and not Mr. Nicolescu on the day of the search?

14 A. Yes.

13:25:12 15 Q. And there were items in that home that belonged to
16 third parties, maybe girlfriends or other people associated
17 with Mr. Nicolescu on the day of the search as well?

18 A. I don't know of any third-party items that were seized
19 during the search warrant.

13:25:31 20 Q. Okay. You don't know if any third, other than?

21 A. Other than Mr. Miclaus.

22 Q. So Mr. Miclaus had personal property and items of
23 electronic property at the home, correct?

24 A. Yes.

13:25:45 25 MR. GOLDBERG: Thank you. Nothing further.

Diaz - Cross/O'Shea

1 THE COURT: Cross-examination, Mr. O'Shea.

2 CROSS-EXAMINATION OF STACY DIAZ

3 BY MR. O'SHEA:

13:26:03

4 Q. Good afternoon, Agent. And again, congratulations on
5 your engagement?

6 A. Thank you.

13:26:17

7 Q. Investigations can lead to lots of places apparently.
8 Now, not being the computer expert that you are, the
9 questions I'm going to ask you are just general questions,
10 not related to necessarily the investigation but just about
11 how computer systems for special network proxies work.

12 As I understand it, let's say that this was a computer
13 here and you've got a computer here, and let's go to this
14 computer over here.

13:26:31

15 If this computer wants to talk to that computer, it
16 can use your computer as a proxy to use that same
17 demonstrative exhibit to communicate to this computer over
18 here, am I right about that?

13:26:47

19 A. Yeah. If this one is set up as a proxy, yes, it
20 could.

21 Q. As a matter of fact, if we take it back further, if
22 you want to get really savvy, you can go three, four, five,
23 six computers out as far as remote and proxies, right?

24 A. Yes.

13:26:59

25 Q. And let's say somewhere in the town where these guys

Diaz - Cross/O'Shea

1 were arrested, there could be a computer that was being used
2 as a proxy for their group as well, am I right about that,
3 and someone could be standing behind that proxy, people you
4 have no idea who they are, am I right about that?

13:27:17

5 **A.** Yes.

6 **Q.** Now, this term, Bayrob Group, just so I'm clear, what
7 set of human beings invented that term "Bayrob"?

8 **A.** Liam Omurchu works for Symantec, and he made named the
9 Bayrob trojan virus.

13:27:47

10 **Q.** Okay.

11 So the name "Bayrob" itself does not come from anybody
12 that's accused of a crime, am I right about that?

13 **A.** That's correct.

14 **Q.** Okay.

13:27:56

15 Now let's talk about this term you heard earlier today
16 and yesterday called malware. And malware, correct me if
17 I'm wrong, Agent Diaz, is where a computer program that you
18 buy or a file that you have takes a file and places it on
19 your computer somewhat without your permission, am I right
20 about that?

13:28:27

21 **A.** It could be that way.

22 **Q.** Would you agree with me that lots of commercial
23 software, including but not limited to Word, Word Perfect,
24 Outlook, they had -- they surreptitiously, without telling
25 people, install minute pieces of software on your computer,

13:28:43

Diaz - Cross/O'Shea

1 am I right about that?

2 **A.** Yes.

3 **Q.** As a matter of fact, there are computer programs out
4 there designed by the computer experts that are called
13:28:53 5 Malware Removal Programs, right?

6 **A.** Yes.

7 **Q.** And the job is to go into the computer and find out
8 wherever your computer may be, what type of uninvited
9 software there might be on your computer, am I right?

13:29:06 10 **A.** Yes.

11 **Q.** And not all malware that's placed on computers is
12 necessarily criminal in nature, some of it's more like
13 marketing base, they want to take optics and metrics, what
14 kind of activities you are, and send them up to marketers
13:29:22 15 and the like, am I right about that?

16 **A.** Generally speaking, malware is malicious software. So
17 it's something that is designed to do something bad to your
18 computer.

19 **Q.** But malware removal programs, correct me if I'm wrong,
13:29:37 20 Agent, look to take out all that commercial stuff that you
21 didn't ask for anyway, am I right about that?

22 **A.** Yes.

23 **Q.** Not necessarily stuff that is criminal, am I right?

24 **A.** Yes.

13:29:46 25 **Q.** Okay. And just so I understand again, rough computer

Diaz - Cross/O'Shea

1 technology is -- I have a laptop here. If I shut my laptop
2 off or -- strike that.

3 If I take my laptop, use it in this courtroom and go
4 say to the Starbucks down the street here on West 6th Street
13:30:17 5 and I log on to the same stuff I was logging on to here,
6 would I have the same IP address?

7 **A.** No.

8 **Q.** Okay.

9 So sometimes your IP address is determined solely not
13:30:28 10 by necessarily the device but by geography, right?

11 **A.** Yes, the Internet connection where you're at.

12 **Q.** All right.

13 And so if you grab someone's laptop and you're not
14 going to be able to say, for instance, I have my laptop with
13:30:45 15 me and two weeks from now, it has a -- I'm somewhere else,
16 it has a different IP address, how do you determine where
17 that computer was on a particular day when you allege a
18 crime occurred?

19 **A.** This is -- I was talking earlier about when I do a
13:31:02 20 subpoena or a search warrant, I need to know the exact date
21 and time so that is -- I have to have a specific IP address
22 on an exact date at an exact time and that is the
23 information that I provide to an Internet service provider,
24 and then they will tell me back who was using that IP
13:31:18 25 address.

Diaz - Cross/O'Shea

1 Q. So if you're a slick kind of criminal fellow and you
2 want to log on from a Starbucks, how do you know, how can
3 you tie that to anybody's particular laptop?

4 A. So the best I could do is I would be able to determine
13:31:32 5 it came from this Starbucks, I would then have to go to the
6 Starbucks. I could look at their server to see if there was
7 any kind of logging on the Starbucks system on their router
8 to determine if there's anything that would help me, but
9 more than anything, I would probably have to get video
13:31:47 10 surveillance to see who was in the Starbucks at that time.

11 Q. Okay. Fair enough.

12 And as I understand it, even if I'm at my home, and
13 say for instance I'm sick of my kids being on the Internet
14 too long, if I shut down that modem and shut it off for long
13:32:06 15 enough, it reassigns a new IP address to it, does it not?

16 A. Yes, it does.

17 Q. How long does it generally have to be shut down before
18 a new IP address is assigned to it?

19 A. I think it depends on the Internet Service Provider.
13:32:21 20 I mean sometimes you can turn it off and turn it back on and
21 get the same IP.

22 Q. Okay.

23 Now, there was some questions asked of you before we
24 broke for lunch about the Bayrob Group and this inventory
13:32:46 25 list that you had in connection with the search. Again,

Diaz - Cross/O'Shea

1 when you answered that question, you just assumed that the
2 Bayrob Group, that was the Bayrob Group stuff because names
3 are placed on that sheet, am I right about that, to be fair?

4 **A.** Not sure I understand.

13:33:06

5 **Q.** For instance, in America, when we execute search
6 warrants in law enforcement, we have the warrant, it's
7 handed to somebody, and -- whose place you might be
8 searching or device you might be searching, and then after
9 the search is over, this thing called an inventory sheet is
10 created, am I right about that?

13:33:19

11 **A.** Yes.

12 **Q.** All right.

13 As it relates to this Romanian version, I don't know
14 what they call it, but an inventory sheet they had, there
15 were names placed on that inventory sheet and various
16 columns and one of them says this is -- this person's stuff,
17 the other says this is the person's stuff, am I right about
18 that?

13:33:30

19 **A.** Well, it's designating the location of the search
20 warrant, and who was associated with that location, yes.

13:33:46

21 **Q.** Got you. But that's based upon what you heard
22 somewhere else or heard from somebody else, am I right about
23 that?

24 **A.** It's based upon lots of different things, records of
25 who was renting the apartment, who -- what relatives lived

13:34:02

Diaz - Cross/O'Shea

1 there and yes, who told us, you know, this person stays
2 here, this person lives there, as well as surveillance
3 conducted by the Romanian National Police.

4 **Q.** Let me ask you this way.

13:34:17 5 If we're doing it the American way and you go to a
6 police and you raid a house and you fill out an inventory
7 sheet, use that inventory sheet somewhere, you place what
8 you believe to be the possessor owner of that particular
9 item, am I right?

13:34:31 10 **A.** Of the item or the location?

11 **Q.** Of the item, sometimes on the sheet themselves?

12 **A.** On an FBI inventory sheet, generally, no, we don't
13 place who the item belongs to.

14 **Q.** Fair enough.

13:34:45 15 So in this regard, the sheets you were talking about,
16 the inventory sheet you were talking about today, just
17 listed for reference people by virtue of their purported
18 residence there, am I right about that?

19 **A.** The fact that they were associated with that location,
13:35:01 20 yes.

21 **Q.** Okay.

22 Well, I live in a house in Rocky River. I assume I'm
23 associated with that location, is that what you mean by
24 that?

13:35:09 25 **A.** Yes.

Diaz - Redirect/Levine

1 Q. Okay.

2 And if I have people in and out of there on a regular
3 basis, would they be associated with that location, too?

4 A. Yes.

13:35:18 5 Q. Okay.

6 MR. O'SHEA: Thank you. Nothing further, your
7 Honor.

8 THE COURT: Redirect?

9 MR. LEVINE: Thank you, your Honor.

13:35:25 10 REDIRECT EXAMINATION OF STACY DIAZ

11 BY MR. LEVINE:

12 Q. All right.

13 I think we got a little confused starting at the end
14 there. Because there are two different kinds of search
15 forms in this case in Romania; isn't that right?

16 A. Yes.

17 Q. So what are the two different kinds of inventory forms
18 that you saw and talked about during your direct and in
19 Romania?

13:35:49 20 A. There was an inventory form for each individual
21 location that was filled out during the search warrant by
22 the Romanian National Police and then signed by the subject
23 that was located at that location, and then --

24 Q. Okay. So let's start with that particular form.

13:36:07 25 A. Okay.

Diaz - Redirect/Levine

1 Q. You saw that form being filled out by -- in Danet's
2 location?

3 A. Yes, I did.

4 Q. Okay.

13:36:14 5 And what was the process by which that form was filled
6 out?

7 A. The Romanian National Police officer sat, as I said
8 earlier, sat down next to Tiberiu Danet and filled out this
9 form with him sitting right there. He wrote down -- the
13:36:29 10 officer wrote down every single item that they had
11 identified as being on the search warrant and they were
12 going to seize. Tiberiu Danet was able to review this list
13 of items and physically see them sitting there in the room
14 being wrapped up in bags and being seized, and he was able
13:36:50 15 to sign the form at the bottom of the form.

16 Q. Okay.

17 And when they wrote down the list of items, did they
18 just describe them or did they include the serial numbers?
19 What kind of level of detail did they have?

13:37:01 20 A. Right.

21 If there was a serial number on the item, they would
22 include the serial number sometimes even the model number.
23 If it was an item that didn't have a serial number, then
24 they would describe it as best they could, using color or
13:37:14 25 maybe like if it was a thumb drive, they might say it's a

Diaz - Redirect/Levine

1 two terabyte or two gigabyte thumb drive or hard drive,
2 those types of description.

3 Q. Okay.

4 And was Danet given an opportunity to indicate if any
13:37:28 5 of those items were not his?

6 A. I believe so. I don't speak Romanian but --

7 MR. GOLDBERG: Objection.

8 THE COURT: Well, I'm going to sustain the
9 objection and strike the last question and answer.

13:37:41 10 BY MR. LEVINE:

11 Q. Okay.

12 So there's this form that, inventory form filled out
13 in each location with the Defendant. Now then is there a
14 second inventory form that you signed?

13:37:52 15 A. Yes.

16 Q. Okay. Tell us what that second inventory form is.

17 A. So the second inventory form was produced by the
18 Romanian Prosecutor which had taken all of the information
19 from each individual inventory forms and combined them into
13:38:07 20 a spread sheet designating all the items that were taken
21 from a particular location associated with each subject.

22 Q. Okay.

23 So what was the source then for the information in
24 that second inventory form that summarized everything?

13:38:25 25 A. The original inventory forms from each individual

Diaz - Redirect/Levine

1 location was the source.

2 **Q.** Okay.

3 I think that clarified the inventory form question.

4 Now --

13:38:35 5 **MR. O'SHEA:** Object to the form of that
6 statement.

7 **THE COURT:** Sustained, sustained.

8 **MR. LEVINE:** Sorry, your Honor.

9 **THE COURT:** Strike the statement. Folks,
13:38:41 10 disregard it.

11 BY MR. LEVINE:

12 **Q.** Okay.

13 So Mr. O'Shea talked about different proxies and he
14 used these computers out here as different proxies and he
13:38:53 15 indicated that the proxies could go out even further so you
16 might have Bogdan Nicolescu's house, and that might be a
17 proxy for something else. Do you recall that?

18 **A.** Yes.

19 **Q.** Okay.

13:39:05 20 Were the Bayrob Group or any member of the Bayrob
21 Group ever identified on the basis of IP address?

22 **A.** No.

23 **Q.** So I -- so the IP address never actually contributed
24 to identifying either Nicolescu or Miclaus?

13:39:23 25 **A.** Not associated with the Bayrob trojan or the Bayrob

Diaz - Redirect/Levine

1 botnet, no.

2 Q. Were you -- let me make the question more clear. Were
3 you ever able to trace the Bayrob trojan or the Bayrob
4 activity by IP address back to Nicolescu or Miclaus?

13:39:47 5 A. No.

6 Q. And as far as you know, was anybody ever able to do
7 that?

8 A. No.

9 Q. And why was that?

13:39:53 10 A. Because they were not accessing any of the Bayrob
11 infrastructure of the Internet connection at their house
12 because they used a directional antenna to connect to
13 someone else's Internet connection, and then they used proxy
14 servers to hide the IP address. They took multiple steps to
15 make sure that we would not be able to identify their IP
16 address at their house.

17 Q. Okay.

18 Did you use other methods to identify Nicolescu and
19 Miclaus?

13:40:34 20 A. Yes.

21 Q. Now we talked a little bit about this in
22 cross-examination about this key to Danet's house. Did the
23 FBI want to make a copy of Danet's key when he came into the
24 United States?

13:40:54 25 A. We had been discussing with the Romanian authorities

Diaz - Redirect/Levine

1 the possibility of them entering his apartment without his
2 knowledge to install either audio equipment, video
3 equipment, or something on his computer so that we could
4 conduct electronic surveillance on him.

13:41:13 5 **Q.** And were the Romanian National Police ever able to do
6 that before -- before you provided the key?

7 **A.** No, they were not.

8 **Q.** Why weren't they able to do that?

9 **A.** Tiberiu Danet had installed on the door to his
13:41:28 10 apartment a secure lock, very similar to locks that are used
11 at banks. And so they were not able to get into his
12 apartment.

13 **Q.** Okay.

14 So what did the FBI do when Danet came through Miami
13:41:49 15 International Airport with respect to that key?

16 **A.** We had confirmed with the Romanian authorities at the
17 airport in Bucharest, Romania, when he left that morning
18 that he had the key in his possession. We had prearranged
19 to have experts in copying keys from the FBI to travel to
13:42:08 20 Miami from headquarters, from Washington, D.C., down to
21 Miami, and we had received a search warrant to be able to
22 copy the key to his apartment while he was being secondaried
23 by Border Patrol.

24 **Q.** And what happened to the key after it was copied?

13:42:26 25 **A.** The -- they made a mold of the key basically right

Diaz - Redirect/Levine

1 there at the airport, which was taken back to Washington,
2 D.C. The individuals that were making the copy of the key
3 were able to use the mold and make a key from that mold. I
4 believe it took them only two days to have the key ready.

13:42:46 5 It just so happened that a Special Agent was traveling
6 to Romania that following weekend from California. So we
7 had the key FedExed from D.C. out to LA where that Special
8 Agent was leaving from, and she hand carried the key to
9 Romania that weekend.

13:43:04 10 **Q.** Okay.

11 And were the Romanian National Police able to use that
12 key to install audio recording devices into Danet's
13 apartment?

14 **A.** Yes, they did.

13:43:13 15 **Q.** And did you -- did the FBI later obtain audio from
16 that audio recording?

17 **A.** Yes.

18 **Q.** And was any of that audio -- did any of that audio
19 recording provide any useful evidence against Danet?

13:43:27 20 **A.** No, it did not.

21 **Q.** Why not?

22 **A.** There was nothing in there that we could hear that was
23 evidentiary in nature. It appeared or it sounded that he
24 either would not discuss Bayrob information inside the
13:43:48 25 apartment or if they were going to discuss anything, they

Diaz - Redirect/Levine

1 would ensure that there was loud music. There was something
2 playing in the background; I believe in case someone was
3 listening.

4 **Q.** Okay. Now, did you ever have a copy of Miclaus' key?

13:44:07 5 **A.** No, we did not.

6 **Q.** And why not? Did Miclaus ever travel to the United
7 States?

8 **A.** No, he did not.

9 **Q.** Okay. Did you ever have a copy of Miclaus' key?

13:44:19 10 **A.** No, we did not.

11 **Q.** Did Nicolescu ever travel to the United States?

12 **A.** No.

13 **Q.** Okay.

14 There was some brief discussion about a person by the
13:44:30 15 name of Alexander Marin, traveled to the United States with
16 Danet; is that correct?

17 **A.** Yes.

18 **Q.** And a question of whether his devices were seized and
19 copied. Were his devices seized and copied?

13:44:44 20 **A.** No, they were not.

21 **Q.** Did you have probable cause to seize or copy Alexander
22 Marin's devices?

23 **A.** No.

24 MR. LEVINE: No further questions, your Honor.

13:45:00 25 THE COURT: Based on those questions?

Diaz - Redirect/Levine

1 MR. GOLDBERG: Nothing on behalf of
2 Mr. Nicolescu.

3 MR. O'SHEA: Nothing here, Judge.

4 THE COURT: You may step down, ma'am.

13:45:07 5 THE WITNESS: Thank you, ma'am.

6 THE COURT: Call your next witness.

7 MR. McDONOUGH: Your Honor, the United States
8 of America would call Yvonne Moon, formally known as Yvonne
9 Liddy.

13:45:53 10 Please step up to the podium, ma'am, and please raise
11 your right hand.

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Moon - Direct/McDonough

1 YVONNE MOON,
2 of lawful age, a witness called by the GOVERNMENT,
3 being first duly sworn, was examined
4 and testified as follows:

13:46:07 5 DIRECT EXAMINATION OF YVONNE LIDDY

6 BY MR. McDONOUGH:

7 Q. Good afternoon. If you could please slide that
8 microphone toward you.

9 Could you please state your name and spell your last
13:46:37 10 name for the benefit of our Court Reporter?

11 A. Yvonne Moon, it's Y-V-O-N-N-E, last name, M-O-O-N.

12 Q. Yvonne, were you previously -- do you have any
13 previous last names?

14 A. Yes. Liddy, L-I-D-D-Y.

13:46:52 15 Q. By whom are you employed?

16 A. University Hospitals.

17 Q. In what capacity?

18 A. I'm the operations manager of nursing.

19 Q. How long have you been operations manager of nursing
13:47:07 20 at University Hospitals?

21 A. I've been in this role for a year and a half. I've
22 been with University Hospitals since 2009?

23 Q. Okay.

24 Can you tell us a little bit about your educational
13:47:19 25 background?

Moon - Direct/McDonough

1 **A.** Yes.

2 I got my associate's degree at Kent State. I went
3 back for my bachelor's at Ohio University, and I am working
4 on my master's right now at Ohio University.

13:47:35 5 **Q.** What did you get your bachelor's in at Ohio
6 University?

7 **A.** Science of nursing.

8 **Q.** Nursing. And what are you working on your master's
9 right now at Ohio University?

13:47:47 10 **A.** Health care administration.

11 **Q.** Okay. Are you a registered nurse?

12 **A.** Yes.

13 **Q.** How long have you been a registered nurse in the State
14 of Ohio?

13:47:56 15 **A.** Since 2010.

16 **Q.** Where did you grow up?

17 **A.** Perry, Ohio.

18 **Q.** Okay. And where is Perry, Ohio, located?

19 **A.** About 40 minutes east of here.

13:48:07 20 **Q.** Okay.

21 What are your duties as an operations manager of
22 nursing at UH?

23 **A.** I oversee two hospitals, the -- it's like a project
24 manager, all new initiatives for the nursing departments. I
13:48:25 25 rule those out and oversee the nursing areas.

Moon - Direct/McDonough

1 Q. Okay. If you could just keep your voice up just a
2 little bit here. I know there's a fan going here.

3 What UH location are you assigned to particular?

4 A. Yes, University Hospitals in Conneaut and also the
13:48:41 5 location in Geneva.

6 Q. Who do you report to in your job?

7 A. The chief nursing officer.

8 Q. Okay.

9 For University Hospitals?

13:48:50 10 A. Yes, Ashley Fortick.

11 Q. Sorry?

12 A. Ashley Fortick.

13 Q. Okay.

14 Are you familiar with a Leadership Ashtabula?

13:49:00 15 A. Yes.

16 Q. What is that?

17 A. It's a leadership group. You are nominated through
18 your employer, and it's a year long project. You learn more
19 about the community, do community service, and then after
13:49:17 20 you finish your year, you partake in different areas and
21 boards in the community.

22 Q. Okay. How long have you been involved in that?

23 A. Since September of 2018.

24 Q. And are you working on any kind of community project
13:49:30 25 now?

Moon - Direct/McDonough

1 **A.** Yes.

2 Right now, we're working on increasing the
3 transportation in Ashtabula County to health care
4 organizations, such as University Hospitals.

13:49:41 5 **Q.** Okay. All right.

6 I want to turn your attention back to October 12th of
7 2007. Do you recall where you were living at the time?

8 **A.** Yes. 476 Eastwood Street in Geneva, Ohio.

9 **Q.** What was your marital status at the time?

13:50:08 10 **A.** I was married.

11 **Q.** Did you have any children at the time?

12 **A.** Yes, two little girls.

13 **Q.** Okay.

14 What were their ages approximately back then?

13:50:22 15 **A.** 2007, my daughter was born in 2007. So she was maybe
16 seven months old. And they're three and a half years apart,
17 so.

18 **Q.** Okay. Did you have Internet access at home?

19 **A.** Yes.

13:50:36 20 **Q.** Do you recall who your provider was?

21 **A.** I don't.

22 **Q.** Okay. What did you use the Internet for?

23 **A.** Well, I was taking classes for school.

24 **Q.** Okay.

13:50:51 25 **A.** So some was for that. And then other than that, it

Moon - Direct/McDonough

1 would have been, I want to say pleasure, whether it was
2 shopping or whatever I was doing on there.

3 **Q.** Okay.

4 When you say classes for school, was that for your
13:51:07 5 BSN?

6 **A.** It was for my associate's.

7 **Q.** Sorry, the associate's degree. Before the bachelors
8 of science?

9 **A.** Yes.

13:51:13 10 **Q.** So online courses?

11 **A.** Yes.

12 **Q.** Have you ever shopped online?

13 **A.** Yes.

14 **Q.** Are you familiar with any shopping websites?

13:51:21 15 **A.** Yes.

16 **Q.** And what shopping website led you in October of 2007?

17 **A.** That would have been eBay.

18 **Q.** Okay.

19 Can you tell us how you are familiar with eBay?

13:51:36 20 **A.** I had used it in the past to make purchases, small
21 purchases, things for my daughter's birthday parties. Back
22 then there wasn't Amazon. So I mean eBay was kind of where
23 you went for anything like that.

24 **Q.** How often would you have used eBay to make purchases?

13:51:56 25 **A.** Probably maybe 20, 25 times prior to that purchase.

Moon - Direct/McDonough

1 Q. Okay. And from who were you buying items on eBay?

2 A. Some were individual sellers, some were companies, a
3 list of things on there.

4 Q. How did you purchase an item on eBay from your home
13:52:20 5 back in 2007?

6 A. You could either do it as an auction or a "buy it
7 now".

8 Q. Okay. Let's talk about the auction. How did the
9 auction process work?

13:52:30 10 A. You would click on the amount and what you wanted to
11 pay for it, and then whether you got outbid before the
12 auction ended, it was like a time frame.

13 Q. Okay.

14 In order to use a bid, did you have to create
13:52:46 15 anything?

16 A. I had an account, yes.

17 Q. So you created an account?

18 A. Um-hum.

19 Q. What was that process? What did you have to do for
13:52:55 20 that?

21 A. Your name, address, linked a credit card to it for
22 your purchases.

23 Q. Okay.

24 And you're doing this on your home computer?

13:53:06 25 A. Yes.

Moon - Direct/McDonough

1 Q. What -- you recall the website address for eBay?

2 A. EBay.com.

3 Q. EBay.com. So you went in there, created an account.

4 You had to put your credit card info in there and your name?

13:53:18 5 Okay.

6 And then you bid -- you say you bid on an item. Did
7 you win, lose, how did that work?

8 A. For the purchases that I made?

9 Q. Yes.

13:53:28 10 A. Some of them, some of them I didn't, and then I'd go
11 back and look for a similar item.

12 Q. Okay.

13 And what was the highest value of the item that you
14 would have purchased?

13:53:40 15 A. Maybe \$100, \$200 at the most.

16 Q. Okay.

17 And then how did the -- how were you -- how did the
18 payment was made for that, through what?

19 A. You could pay it automatically through eBay with the
13:53:55 20 card that was linked or you could use PayPal, which was
21 something else that was linked to mine.

22 Q. What is PayPal?

23 A. Like an online -- you store your credit card in there
24 and you can make purchases through eBay. That was kind of
13:54:12 25 how things used to be.

Moon - Direct/McDonough

1 Q. Okay.

2 A. I don't know how much people use PayPal anymore.

3 Q. PayPal, did you have to create an account?

4 A. Yes.

13:54:22 5 Q. Same thing?

6 A. Name, address, and a credit card number. I think you
7 could link your checking account as well.

8 Q. You could put your bank account information? What
9 bank were you doing your banking back in October of 2007?

13:54:36 10 A. First Merit.

11 Q. First Merit. Where was First Merit located?

12 A. The branch that I used was about a mile from my street
13 or where I lived, down the street from me. It was on South
14 Broadway in Geneva.

13:54:50 15 Q. And Geneva is located in what county?

16 A. Ashtabula County.

17 Q. And Ashtabula County is located in Northeastern Ohio?

18 A. Yes.

19 Q. You mentioned that on eBay, there was a second option,
13:55:03 20 a "buy it now" option. How did that work?

21 A. Basically the item was your if you select the "buy it
22 now." So sometimes you paid a little bit more if it was a
23 smaller item than you would if it was an auction, but you
24 were guaranteed the item.

13:55:23 25 Q. Were you ever successful in using "buy it now"?

Moon - Direct/McDonough

1 **A.** Yes.

2 **Q.** What did you buy?

3 **A.** What I remember, because this was awhile ago, was
4 birthday party supplies for my daughters' parties.

13:55:36 5 **Q.** Okay.

6 Did you ever have any issues with either the auction
7 for the "buy it now" on any of those smaller purchases?

8 **A.** No, and I always looked at the ratings of the people
9 before I purchased, too.

13:55:53 10 **Q.** When you say that you looked at the ratings, could you
11 describe -- what are you looking at or what do you mean by
12 that?

13 **A.** When you have a user name like in the -- for eBay, if
14 you're a seller, it will show how your transactions went,
13:56:06 15 like the people that buy things from you, rate you.

16 So, you know, if you did everything right, it will say
17 you're 100 percent or 95 percent or whatever. If you've
18 made bad transactions, it'll show you, you know, that
19 feedback as well.

13:56:19 20 **Q.** Okay.

21 Did you review the ratings of sellers before you made
22 purchases?

23 **A.** Sure, it was right up in the corner.

24 **Q.** Did you ever decide not to make a purchase based on
13:56:33 25 someone having a bad rating?

Moon - Direct/McDonough

1 **A.** Sure.

2 **Q.** Okay.

3 And what was the rating scale? Was it stars, numbers,
4 or diamonds?

13:56:40 5 **A.** It was numbers. It was like up to 100 percent.

6 **Q.** Up to 100. Okay. All right.

7 What was your automobile situation like in October of
8 2007?

9 **A.** We were looking for a new family vehicle.

13:56:57 10 **Q.** Okay. And when you say we, you --

11 **A.** My husband and I.

12 **Q.** Okay. What vehicle were you looking for?

13 **A.** Well, something that could fit two car seats.

14 I liked the Jeep Liberty, which was kind of
13:57:15 15 specifically what I was looking for at the time.

16 **Q.** You were looking for a Jeep Liberty?

17 **A.** Um-hum.

18 **Q.** An automobile?

19 **A.** Yes.

13:57:21 20 **Q.** How were you able to find the Jeep Liberty on eBay?

21 **A.** Just putting it in the search engine and looking for
22 what I wanted.

23 **Q.** When you say search engine, you went to the eBay site?

24 **A.** Yes.

13:57:40 25 **Q.** And when you say --

Moon - Direct/McDonough

1 **A.** Like a specific area for auto sales or auctions, and
2 you could just type in what you wanted. You could put the
3 year, mileage, you -- yeah.

4 **Q.** Did you do a search for Jeep Liberty?

13:57:59 5 **A.** I think I put Jeep. I don't know if I was specific to
6 Liberty.

7 **Q.** Did you find a jeep you liked?

8 **A.** Yes.

9 **Q.** How could you see what the jeep looked like?

13:58:08 10 **A.** There's pictures and a description.

11 **Q.** Okay. Did you view the pictures?

12 **A.** Yes.

13 **Q.** Did you read the description?

14 **A.** Yes.

13:58:15 15 **Q.** Based on that, what did you then do?

16 **A.** I called my husband, who knows a little bit more about
17 cars than I do, and had him look it over.

18 **Q.** Okay.

19 And without telling me what your husband said, did
13:58:29 20 your husband have a chance to look it over?

21 **A.** Yes.

22 **Q.** Did you -- and based on that conversation, did you end
23 up putting a bid on a jeep?

24 **A.** Yes.

13:58:38 25 **Q.** Okay.

Moon - Direct/McDonough

1 Were you -- and was it the auction or was it the "buy
2 it now"?

3 **A.** Well, it was originally the auction.

4 **Q.** Okay.

13:58:46 5 **A.** But then the auction ended, we didn't hear anything.

6 **Q.** Okay.

7 Did you know where -- were you successful in the
8 auction?

9 MR. O'SHEA: Objection.

13:58:58 10 THE WITNESS: I don't remember.

11 **Q.** Okay.

12 Do you remember whether that car -- whether a reserve
13 was met?

14 **A.** No.

13:59:13 15 **Q.** What's a reserve?

16 **A.** The lowest amount that the seller will take for the
17 car, whatever the item is.

18 **Q.** Did you receive any communications regarding that
19 jeep?

13:59:25 20 **A.** Yes, after the auction had ended.

21 **Q.** Okay. Let me ask you this.

22 Do you remember the time that you're looking at photos
23 of the jeep, reading the description, did you have any
24 communications with the seller?

13:59:45 25 **A.** Yes, I sent some questions and asked some -- for some

Moon - Direct/McDonough

1 more details regarding the vehicle.

2 Q. Are you familiar with the seller by the user name of
3 Brown44J, Brown44J?

4 A. Yes.

14:00:04 5 Q. How are you familiar with that user name?

6 A. That's what the vehicle was listed under.

7 Q. Okay. That was the seller?

8 A. Um-hum.

9 Q. Was that a yes?

14:00:14 10 A. Yes.

11 Q. Okay. How did you communicate with the seller?

12 A. E-mail.

13 Q. Okay.

14 And was that e-mail through eBay or through some other
15 e-mail program?

16 A. It lists the contact, like you could click on it to
17 message the seller. So it started, yeah.

18 Q. Started through eBay?

19 A. Yes.

14:00:36 20 Q. What type of questions did you ask the seller?

21 A. Just what I remember was just like whether it was in
22 good condition and if they -- there was any issues with the
23 vehicle. I don't -- I don't remember specific more than
24 that.

14:00:51 25 Q. Okay.

Moon - Direct/McDonough

1 Do you recall the reason the seller was selling the
2 vehicle?

3 **A.** A divorce.

4 **Q.** Do you recall what the rating of the seller was?

14:00:59 5 **A.** 100 percent.

6 **Q.** Okay.

7 After that auction ended, you said you didn't hear
8 anything, correct?

9 **A.** That's correct.

14:01:11 10 **Q.** What was your next contact with brown44J?

11 **A.** I received an e-mail.

12 **Q.** Okay.

13 **A.** Saying that the car was going to be listed again as a
14 "buy it now".

14:01:23 15 **Q.** Okay. So a second opportunity?

16 **A.** Yes.

17 **Q.** Was there a reason given as to why the car didn't sell
18 the first time?

19 **A.** Just that the reserve wasn't met.

14:01:33 20 **Q.** Okay.

21 So now on the second opportunity, did you do the "buy
22 it now"?

23 **A.** Yes.

24 **Q.** Okay.

14:01:41 25 Can you describe what was the process to do the "buy

Moon - Direct/McDonough

1 it now" the second time around?

2 **A.** It was pretty simple. I went in and found the vehicle
3 and clicked the "buy it now."

4 **Q.** Okay.

14:01:54 5 And you clicked on the "buy it now" and what was the
6 information on there?

7 **A.** As far as the vehicle or --

8 **Q.** Do you recall how much the price was?

9 **A.** \$8600.

14:02:15 10 **Q.** \$8650?

11 **A.** That sounds correct.

12 **Q.** Sounds about right?

13 **A.** Yes.

14 **Q.** How were you going to go ahead and pay that amount?

14:02:23 15 **A.** It was supposed to be a wire transaction. So I had to
16 go to First Merit and take money out of my savings and
17 transfer it.

18 **Q.** Okay.

19 Had you ever done a wire transaction before for eBay?

14:02:39 20 **A.** No.

21 **Q.** Okay.

22 Do you recall looking at any pictures of the Jeep
23 Liberty?

24 **A.** Yes.

14:02:48 25 **Q.** And what pictures would you have seen of the Jeep

Moon - Direct/McDonough

1 Liberty?

2 **A.** The pictures on eBay, and then I received an e-mail
3 with additional pictures.

4 **Q.** Okay.

14:02:58 5 I want to ask about that e-mail that you received with
6 the additional pictures.

7 When did you receive the e-mail with the additional
8 pictures? Was that after the auction?

9 **A.** After the initial auction.

14:03:19 10 **Q.** Was that before the "buy it now"?

11 **A.** Yes.

12 **Q.** When -- did you click on the attachment with the
13 pictures?

14 **A.** Yes.

14:03:29 15 **Q.** And when you did that, what did you see?

16 **A.** Pictures of the vehicle.

17 **Q.** And can you describe what those pictures looked like
18 of the vehicle?

19 **A.** It was a white Jeep Liberty and it showed pictures of
14:03:46 20 different angles, and I mean that was -- there was a handful
21 of pictures that went through, like you would see now when a
22 dealer listed a vehicle.

23 **Q.** Exterior pictures?

24 **A.** Yes.

14:04:00 25 **Q.** Interior pictures?

Moon - Direct/McDonough

1 **A.** I believe so.

2 **Q.** Did it indicate the mileage?

3 **A.** The mileage was listed on the listing. I don't know
4 that there was a specific picture.

14:04:10 5 **Q.** You heard of something called Carfax?

6 **A.** Yes.

7 **Q.** What's Carfax?

8 **A.** Well, what I would say I would look at it for is to
9 see if the car was in an accident or it was true to the
14:04:21 10 mileage.

11 **Q.** Okay. How did that Jeep Liberty look in the
12 photographs?

13 **A.** Like it was described in the auction.

14 **Q.** Okay.

14:04:33 15 So you clicked on the "buy it now" and you had a wire
16 transfer option. Can you describe how did you find out
17 about the wire transfer option?

18 **A.** Through communication with the seller.

19 **Q.** Okay.

14:04:48 20 **A.** But that was the process.

21 **Q.** And that the process would be you have to wire
22 transfer?

23 **A.** Yes.

24 **Q.** Did you have any concerns at that point?

14:04:58 25 **A.** Everything seemed legitimate to me. The pictures were

Moon - Direct/McDonough

1 there. It was on eBay. My husband actually has known
2 people that have done auctions online. So it didn't seem
3 out of the norm to us.

4 **Q.** You trusted the seller?

14:05:16 5 **A.** Yes, and the site.

6 **Q.** Okay.

7 Describe what you did when you went to First Merit
8 Bank in Geneva?

9 **A.** I asked the teller how to do the wire transfer because
14:05:32 10 I haven't done that before. She told me that I needed the
11 information of where it was going and what bank and where
12 at. And then I had to withdraw my money out of my savings
13 and fill out additional paperwork to have it wired to the
14 Washington Mutual Bank.

14:05:55 15 **Q.** Where did you get the information of where to wire
16 your money from your account, which is at First Merit in
17 Geneva, was it Washington --

18 **A.** Mutual.

19 **Q.** Mutual Bank? What state is Washington Mutual Bank?
14:06:15 20 Is it outside the State of Ohio?

21 **A.** Yes, it was California.

22 **Q.** California.

23 So for the wire transfer to go from Ohio to
24 California, where did you get the information on the -- on
14:06:26 25 where to send the wire transfer to?

Moon - Direct/McDonough

1 **A.** The communication with the seller.

2 **Q.** Okay. Do you recall the name of Amber Gallegos?

3 **A.** Yes.

4 **Q.** G-A-L-L-E-G-O-S?

14:06:41 5 **A.** Yes.

6 **Q.** How do you recognize that?

7 **A.** That was the seller.

8 **Q.** Okay.

9 You had -- did you receive account number information
14:06:53 10 or routing account information as to that Washington Mutual
11 Bank?

12 **A.** Yes.

13 **Q.** Okay.

14 Do you know where the Jeep Liberty was located?

14:07:07 15 **A.** It was hers, and that's the address. So it was coming
16 from California. It was being shipped.

17 **Q.** Okay.

18 Did you provide the information to your bank for this
19 Amber Gallegos with the bank account information for
14:07:27 20 Washington Mutual Bank?

21 **A.** Yes.

22 **Q.** How did the wire transfer proceed? You have to --

23 **A.** I gave them the information, I signed off on it, and
24 they removed the money from my account and sent it to hers.

14:07:39 25 **Q.** Was \$8650 a significant amount of money for you at

Moon - Direct/McDonough

1 that time?

2 **A.** At that time, it was. I was a stay-at-home mom and a
3 student, and yes.

4 **Q.** Okay. Did you ever get the Jeep Liberty?

14:08:00 5 **A.** No.

6 **Q.** What happened?

7 **A.** Well, I believe I was supposed to get an e-mail or a
8 confirmation of shipping, I want to say early in the week.

9 And by Wednesday, I started to get nervous that something
14:08:17 10 wasn't right, and the -- the seller wasn't answering.

11 **Q.** Okay.

12 When you say by Wednesday, was that Wednesday of the
13 week following the wire transfer?

14 **A.** Yes.

14:08:26 15 **Q.** That had posted to your account?

16 **A.** Yes, so the money was gone but I hadn't received a
17 shipping confirmation.

18 **Q.** Okay.

19 Did you have any understanding as to whether you would
14:08:37 20 be able to inspect the vehicle?

21 **A.** I don't recall that.

22 **Q.** You mentioned you contacted the seller. How did you
23 try to contact the seller?

24 **A.** Initially through e-mail. And then I started
14:08:55 25 searching on the Internet to find her to see if I could find

Moon - Direct/McDonough

1 a different contact number. I mean that was a lot of money
2 and I hadn't heard from anybody.

3 **Q.** Okay.

4 How did you search on the Internet to find the
14:09:09 5 seller's phone number?

6 **A.** I put in her name.

7 **Q.** Okay.

8 **A.** Where she lived, hit search, and looked until I found
9 something.

14:09:19 10 **Q.** And did you find something?

11 **A.** I found a phone number.

12 **Q.** Were you able to talk to this Amber Gallegos?

13 **A.** Yes.

14 **Q.** Okay.

14:09:34 15 Without telling me what she said, based on that
16 conversation with Amber, what did you do?

17 **A.** I went to the police department at that point.

18 **Q.** Okay.

19 Which police department did you go to?

14:09:49 20 **A.** Geneva.

21 **Q.** Okay.

22 What did you do at the Geneva police department?

23 **A.** I brought all that I had to them. I mean just -- like
24 the auction that said that I won and the communication and
14:10:06 25 filed a police report and --

Moon - Direct/McDonough

1 Q. Okay.

2 Are you familiar with the IC3 or Internet Crime
3 Complaint Center?

4 A. Yes.

14:10:16 5 Q. How are you familiar with that?

6 A. Again, I felt hopeless when I got home. I didn't
7 really get anywhere when I was at the Geneva police
8 department. So I continued to search what else I could do
9 at this point, and that was what I came across.

14:10:33 10 Q. When you said you felt helpless at the Geneva police
11 department, what did you mean by that?

12 A. They're a small local police department, and I -- they
13 didn't really have any jurisdiction over eBay or any of the
14 situation. I mean they made a couple calls just to the bank
14:10:52 15 and whatever for me, but there wasn't much they could do.

16 It was out of their hands.

17 Q. Did you go to First Merit?

18 A. I did.

19 Q. What did you try to do at First Merit?

14:11:02 20 A. To stop or return the money, but it was too late.

21 Q. Okay.

22 Could they reverse the transaction somehow?

23 A. They said no.

24 Q. Did you contact eBay?

14:11:15 25 A. Yes.

Moon - Direct/McDonough

1 Q. Okay. How did you contact eBay?

2 A. Just through their -- there's like a link on there
3 that you can send a message to them regarding purchases or
4 feedback, whatever. That's how I contacted them.

14:11:35 5 Q. Did you get any response from eBay?

6 A. That it was not --

7 MR. GOLDBERG: Objection.

8 MR. O'SHEA: Objection.

9 THE COURT: Just yes or not, ma'am.

14:11:45 10 THE WITNESS: Yes.

11 Q. Based on that response from eBay, what did you do?

12 A. Well, that's when I started doing more searches and
13 figuring out what I could do.

14 Q. You mentioned earlier you have an account with eBay,
14:12:03 15 user account. Are you familiar with the My Won portion of
16 your account?

17 A. The My One?

18 Q. My Won, or Auctions Won?

19 A. Oh, Auctions Won, yes.

14:12:13 20 Q. Okay. Auctions Won?

21 A. Yes.

22 Q. What is Auctions Won?

23 A. It shows you what you've won and what you've purchased
24 in the past.

14:12:21 25 Q. Regarding the Jeep Liberty, did that show up in your

Moon - Direct/McDonough

1 Auctions Won?

2 MR. GOLDBERG: Objection.

3 THE WITNESS: Yes.

4 THE COURT: Overruled.

14:12:33 5 THE WITNESS: Yes, at my home computer.

6 Q. From which computer?

7 A. My home computer.

8 Q. Did you go on any other computer to the eBay site and
9 lot into your account?

10 A. Yes.

11 Q. What other computer did you go to?

12 A. I tried to show them at the police department.

13 Q. Geneva?

14 A. Yes.

14:12:56 15 Q. Were you able to access your eBay account from the
16 Geneva police department?

17 A. Yes. But the auction wasn't there.

18 Q. When you said the Auctions Won --

19 A. Yes.

14:13:05 20 Q. -- were you able to access that?

21 A. Yes, but the vehicle wasn't listed on there.

22 Q. Jeep Liberty wasn't listed on there at all?

23 A. No.

24 Q. Did you relay that information to eBay?

14:13:17 25 A. Yes.

Moon - Direct/McDonough

1 Q. You mentioned you went online to do a little research
2 regarding feeling helpless at Geneva. Did you end up filing
3 a complaint with the IC3, Internet Computer Crime Center?

4 A. I did.

14:13:48 5 Q. What information did you provide?

6 MR. O'SHEA: Objection. For a second, can I
7 ask Mr. McDonough something?

8 THE COURT: Certainly.

9 (Counsel conferring.)

14:14:36 10 MR. O'SHEA: Thank you, Judge.

11 THE COURT: Sure.

12 Q. You went ahead and filed the complaint on the Internet
13 Crime Complaint Center?

14 A. I did.

14:14:41 15 Q. And you provided all the information that you had
16 regarding that?

17 A. Yes.

18 Q. Regarding this transaction? Okay.

19 Did you ever have a chance to talk to the Cleveland
14:14:58 20 FBI?

21 A. Yes.

22 Q. Okay.

23 On October 12th, 2007, did you contact the Cleveland
24 FBI?

14:15:07 25 A. Yes.

Moon - Direct/McDonough

1 Q. How did you do so?

2 A. I believe I called and I had sent an e-mail.

3 Q. Okay.

4 Did the Cleveland FBI respond to your call?

14:15:18 5 A. Yes, they actually came to my home.

6 Q. Cleveland FBI came to your house. Do you know someone
7 by the name of Special Agent Diaz, formerly known as Special
8 Agent Stacy Lough?

9 A. I do.

14:15:31 10 Q. Do you see her here in the courtroom today?

11 A. Yes, she's --

12 Q. Could you please point her out and --

13 MR. O'SHEA: We stipulate that's Agent Diaz,
14 your Honor.

14:15:42 15 MR. McDONOUGH: Okay. We'll accept the
16 stipulation, your Honor.

17 Q. Did you have your computer at home?

18 A. I did.

19 Q. Did you provide a consent for the FBI to go ahead and
14:15:55 20 search your computer?

21 A. I did.

22 Q. Did the FBI make a copy of your hard drive?

23 A. Yes.

24 Q. Did you provide the FBI with the information you had
14:16:07 25 provided Geneva police department, eBay, First Merit Bank,

Moon - Direct/McDonough

1 and this IC3 online complaint referral?

2 **A.** Yes.

3 **Q.** Okay. Provided all that information to the FBI?

4 Okay.

14:16:25 5 Have you ever heard of US Wire Services?

6 **A.** Yes.

7 **Q.** What is US Wire Services?

8 **A.** That was where Amber Gallegos said that she had worked
9 or that was the company that she worked for.

14:16:49 10 **Q.** Okay. You mentioned earlier this user, brown44J?

11 **A.** Yes.

12 **Q.** That was what you believed to be the seller of the
13 vehicle?

14 **A.** Yes.

14:17:03 15 **Q.** Was Amber Gallegos the seller of the vehicle?

16 **A.** She -- no.

17 **Q.** Okay.

18 Do you know after you wire transferred the money to
19 Amber Gallegos, where your money ended up?

14:17:20 20 **A.** She works for US Wire Services is what she --

21 MR. O'SHEA: Objection.

22 THE COURT: Sustained.

23 **Q.** After the FBI copied your computer, did you ever end
24 up using that computer again?

14:17:54 25 **A.** No.

Moon - Direct/McDonough

1 Q. Why not?

2 A. Well, obviously, there was a virus on it and I didn't
3 want to use it to do any transactions or anything else that
4 I would be doing on it.

14:18:08 5 Q. Okay.

6 And to date, did you ever get back the \$8650 that you
7 had spent on the jeep in this case?

8 A. I did not.

9 MR. McDONOUGH: No further questions.

14:18:23 10 THE COURT: Mr. Goldberg, cross?

11 MR. GOLDBERG: Thank you, your Honor. I have
12 no questions for Ms. Liddy. Thank you for your time.

13 THE COURT: Mr. O'Shea.

14 MR. O'SHEA: No questions, your Honor.

14:18:31 15 THE COURT: You may step down, ma'am. Watch
16 your step. Call your next witness.

17 MR. LEVINE: Your Honor, the United States
18 calls Chris Drake to the stand.

19 THE COURT: Please step up to the podium, sir.
14:18:55 20 Right up to the podium. Right there. And if you would
21 please raise your right hand.

22

23

24

25

Drake - Direct/Levine

1 CHRISTOPHER DRAKE,
2 of lawful age, a witness called by the GOVERNMENT,
3 being first duly, was examined
4 and testified as follows:

14:19:50 5 DIRECT EXAMINATION OF CHRISTOPHER DRAKE

6 BY MR. LEVINE:

7 THE COURT: Sir, please take a seat right over
8 there. Right up here.

9 MR. LEVINE: Sorry.

14:19:58 10 Q. Can you please state and spell your name for the
11 record?

12 A. Christopher Drake, C-H-R-I-S-T-O-P-R-E-R, D-R-A-K-E.

13 Q. Okay. And what do you do, Mr. Drake?

14 A. I work on and operate the e-mail tracking business
14:20:16 15 called readnotify.com.

16 Q. Okay. That's readnotify.com?

17 A. Yes.

18 Q. Okay.

19 Read Notify is one word?

14:20:24 20 A. That's right.

21 Q. And where are your offices located?

22 A. In Australia.

23 Q. So did you travel from Australia to testify here
24 today?

14:20:34 25 A. I did, yes.

Drake - Direct/Levine

1 Q. How long did it take you to get from Australia to
2 here?

3 A. So it was 26 hours on three different flights and a
4 lot of waiting around in airports in between all those.

14:20:48 5 Q. Oh, my goodness. Well we really appreciate you flying
6 all the way over here for this. Were we able at least to
7 give you an upgrade?

8 A. You were, thanks. I managed to get a bit of sleep on
9 some of those legs.

14:21:00 10 Q. All right. Thank you. All right.

11 I want to talk about Read Notify. So what is
12 readnotify.com?

13 A. We are an e-mail tracking business. So we tell our
14 customers when e-mails they send get opened and often where
14:21:19 15 the recipient is when they open their e-mail.

16 Q. All right.

17 So in order to send a Read Notify e-mail, do you have
18 to be using a Read Notify e-mail account? For example, I
19 have to be BrianLevine@readnotify.com?

14:21:36 20 A. No.

21 Q. What e-mail account could you use?

22 A. You can use any e-mail account you like. It just
23 works with whatever normal e-mail you already use.

24 Q. So if I use a Gmail account, I could use it with that?

14:21:49 25 A. Anything, yes.

Drake - Direct/Levine

1 Q. America Online?

2 A. That's right.

3 Q. Okay.

14:22:00 4 So to say my e-mail was BrianLevine@yahoo.com and I
5 wanted to use Read Notify to send an e-mail, how would I do
6 that?

7 A. So if you wanted to send a tracked e-mail with our
8 service, first of all, you would have to create an account
9 on our service, which is a web page. And after you've done
14:22:13 10 that, you then write an e-mail saying -- you normally would,
11 if you were writing, for instance, to Chris@hotmail.com,
12 you'd compose your e-mail to
13 Chris@hotmail.com.readnotify.com. So you'd add dot
14 readnotify.com on the end --

14:22:30 15 THE COURT: Sir, if you would slow down just a
16 little bit. Maybe you need to repeat a little bit of what
17 you said.

18 THE WITNESS: Oh, sorry.

19 You compose the e-mail as you normally would, and you
14:22:41 20 add the name of my service, which is dot readnotify.com,
21 onto the end of the recipient's e-mail before you hit send.
22 And that's all you have to do for our service to then add
23 the tracking to the e-mail for you.

24 Q. All right.

14:22:54 25 So, in other words, if I was sending an e-mail to

Drake - Direct/Levine

1 just, let's say, recipient@gmail.com, I would send it to
2 just the same -- I would always do except
3 recipient@gmail.com.readnotify.com?

4 **A.** That's right.

14:23:10 5 **Q.** All right.

6 And could the recipient tell I was sending it from
7 readnotify.com or through Read Notify?

8 **A.** Typically not. Our system removes that bit before
9 it's delivered so it looks normal to the recipient.

14:23:23 10 **Q.** Okay.

11 So say I sent the e-mail, what different e-mail would
12 I get back?

13 **A.** So when the e-mail is transmitted, we tell you the
14 information about how it got to the recipient and then when
14:23:36 15 it's opened by the recipient, our system will tell you the
16 date and time in whatever time zone you chose when you
17 signed up that the e-mail was opened, it will tell you the
18 approximate location of person who's opened it, the IP
19 address of the computer they're using and the kind of
14:23:55 20 computer and software the computer is using.

21 **Q.** Could it determine would you -- would your system let
22 the user know whether the person has actually read it? Can
23 it tell whether the e-mail's been read or not?

24 **A.** We differentiate between opening and reading, and if a
14:24:16 25 sender has elected to ask the recipient to confirm reading,

Drake - Direct/Levine

1 then our system will do that and this way, you'll get --
2 part of the receipt you get will be the time it was opened
3 and the time the recipient confirmed reading and
4 understanding the e-mail.

14:24:31 5 **Q.** Okay.

6 But, in that instance, the recipient would know they
7 were being asked to answer a question about whether it was
8 read or not?

9 **A.** That's right.

14:24:39 10 **Q.** All right.

11 What about would you get an alert or would you --
12 would the sender of an e-mail let you know whether the user
13 who receives the e-mail clicks on an attachment to that
14 e-mail?

14:24:54 15 **A.** So we independently track e-mail attachments as well.
16 So depending on what kind of attachment that you've sent,
17 our system will tell you -- let's say it's an Adobe PDF like
18 an Acrobat document, it will tell you when that document was
19 opened, how long they read each page for, and what the pages
14:25:14 20 were that they read as well. That works with Office
21 documents and sort of different file formats, too.

22 **Q.** So you said how long each page was read for. What do
23 you mean by how long each page was read for?

24 **A.** So if you have the server three-page document and you
14:25:33 25 took a minute reading the first page before you went to the

Drake - Direct/Levine

1 second page, we record all of those times. And then we
2 report the amount of time you spent on each page back to the
3 sender.

14:25:44 4 **Q.** Okay. But just so we understand that this is not that
5 creepy, you're looking at the amount of time each page is
6 visible, not necessary -- you can't tell whether they're
7 actually reading it or not?

8 **A.** Just how long it's been opened for on the computer.

9 **Q.** Okay. Just want to make sure.
14:25:58 10 What about clicking on a link? If I were to send an
11 e-mail using Read Notify and there's a link in my e-mail,
12 would Read Notify let me know if the user who receives it
13 clicked on the link?

14 **A.** Yes, every link that you click on, we will tell the
14:26:15 15 sender what link it was, you clicked on, also what time you
16 did that, of course, and the kind of computer you were using
17 to visit that link with.

18 **Q.** Okay.

19 What if -- what if I send an e-mail using Read Notify
14:26:30 20 to you, and you forward it to somebody else, will it
21 indicate to me whether you forwarded the e-mail?

22 **A.** Yes. We record when e-mails have been forwarded as
23 well. We do that by detecting whether the person that
24 originally opened the e-mail is different from a subsequent
14:26:49 25 opening of the same e-mail. So we report if the same person

Drake - Direct/Levine

1 opens the same e-mail many times, differently from when --
2 if a different machine has been used to open that other
3 e-mail, and if it's a different machine, we call that
4 forwarded. And we then report all the information about
14:27:04 5 that second machine so the geolocation, different IP
6 address, different software and so on.

7 **Q.** Okay.

8 I don't want you to reveal any trade secrets here, but
9 on a general level, how is Read Notify able to get all this
14:27:17 10 information?

11 **A.** It's a fairly common thing. Almost all e-mail does it
12 these days. E-mail arrives in a format called HTML, which
13 is just a way of making words and pictures look pretty on
14 the screen when it shows up. So our system puts an
14:27:34 15 invisible image and a silent sound into your e-mail. So
16 when your e-mail program tries to show you the message, it
17 will then go to our server to get the invisible image and
18 the sound, and the fact that our server is being looked up
19 for those images allows us to know that the e-mail that
14:27:52 20 contained them has been opened.

21 **Q.** So, in other words, if I open up an e-mail sent
22 through Read Notify, there is information and e-mail that
23 tells it to check back at your server?

24 **A.** That's right. Every e-mail that goes through our
14:28:07 25 system has a unique code associated with it. And it's that

Drake - Direct/Levine

1 unique code in the image of the sound look up, which let's
2 us know which e-mail it was and who it got sent to.

3 **Q.** So my e-mail thinks it's looking, it's looking to your
4 server for what that picture and sound is?

14:28:25 5 **A.** That's right.

6 **Q.** And do you send back some kind of image or sound?

7 **A.** So the image that we send back, technically it's
8 transparent. So it will just be the same color, whatever
9 the background of your e-mail is. And some people turn
10 images off, which is the purpose of the silent sound. So if
11 you got images turned off, it will still play the sound that
12 doesn't make a noise.

13 **Q.** Okay.

14 So is this -- is this a service that anybody can
15 subscribe for?

16 **A.** Yes.

17 **Q.** And roughly, how much does it cost to use Read Notify?

18 **A.** So we let people use it for 25 e-mails or two weeks
19 for free. And to continue using it after that time, we
14:29:04 20 charge \$3.99 a month or 24 or \$36 a year, depending on if
21 you want advanced features.

22 **Q.** Okay.

23 And roughly, when do you start Read Notify?

24 **A.** We -- I read the code in the Year 2000. Then we
14:29:24 25 started with our first customers in 2001.

Drake - Direct/Levine

1 Q. Okay.

2 And at some point, did you start your own informal
3 investigation into the group that we've been referring to as
4 the Bayrob Group?

14:29:35 5 A. Yes.

6 Q. Roughly, when was that?

7 A. It was approximately 2007.

8 Q. Okay.

9 And what caused you to start investigating the Bayrob
14:29:48 10 Group?

11 A. We had a spike of new customer sign ups using stolen
12 credit cards through our service.

13 THE COURT: One moment. Sir, would you repeat
14 that one more time.

14:30:03 15 THE WITNESS: We had a number of -- we had a
16 spike of new customer sign ups using stolen credit cards to
17 open up accounts with our service.

18 THE COURT: Overruled. I'm going to allow
19 that to stand.

14:30:16 20 MR. LEVINE: Okay.

21 Q. Okay.

22 And not to be callous, but why do you care that
23 someone's using stolen credit cards as long as you're
24 getting paid?

14:30:26 25 THE COURT: Mr. Levine, I have apologize.

Drake - Direct/Levine

1 Didn't someone object.

2 MR. O'SHEA: I did.

3 THE COURT: Yeah.

4 Shirle, I don't think the objection is showing up.

14:30:38 5 MR. O'SHEA: Thank you.

6 THE COURT: I'm sorry, Mr. Levine.

7 BY MR. LEVINE:

8 **Q.** My question is just why -- why did you care that --
9 first of all, how did you know they were users using --

14:30:49 10 **A.** When someone using a credit card without authority to
11 open an account with us, we suffer what's called a charge
12 back, which is when our payment provider gets the complaint
13 from the real card holder saying this wasn't me buying that
14 service, and they'll take back the money we got for it, plus
14:31:09 15 they'll charge an extra \$50 penalty for having accepted a
16 stolen, improper, whatever the cause is for that card --

17 **Q.** Really?

18 **A.** -- not to have been approved.

19 **Q.** Is that -- so you get charged \$50 every time you
14:31:25 20 accept a credit card that turns out to be stolen?

21 **A.** Yes.

22 **Q.** Is that an Australia rule or is that in general?

23 **A.** We use a payment provider called World Pay, which is a
24 UK business, and that's just the way that their system
14:31:44 25 approaches.

Drake - Direct/Levine

1 Q. So you're being charged \$50 every time a fake credit
2 card was used?

3 A. That's right.

14:31:57

4 Q. And at a general level, what did you do to investigate
5 the Bayrob Group?

14:32:16

6 A. So when we started getting a lot of charge backs all
7 at once, I looked into why this was happening. We initially
8 started cancelling the accounts that were having stolen or
9 causing charge backs through them, but unfortunately, this
10 caused them to open new accounts and use more credit cards,
11 which caused more charge backs. So it was costing us too
12 much money to keep cancelling the new accounts. So I
13 investigated what they were doing with their accounts.

14 Q. Okay.

14:32:29

15 And did you attempt to find all the accounts that this
16 person or group was setting up?

17 A. Yes.

18 Q. Okay. And how did you do that?

14:32:45

19 A. Over the course of many years, the methods I used
20 evolved. So originally it was looking for all accounts that
21 had had a charge back associated with them. And then that
22 evolved to looking at the names that were used by the people
23 opening the accounts and the e-mail addresses that we used.
24 Later on, I started looking at the way that they were using
14:33:05 25 the accounts, the kinds of e-mails software that they were

Drake - Direct/Levine

1 using, and subject lines of their e-mails.

2 Q. All right.

3 And I want to show you -- if we can show just --
4 actually, I'm going to hand you Government's Exhibit 1321.

14:33:42 5 MR. O'SHEA: Let me catch up with you.

6 BY MR. LEVINE:

7 Q. What is Government's Exhibit 1321?

8 A. This is an e-mail that I write to Stacy explaining how
9 I was detecting the accounts that were being used.

14:34:01 10 Q. Okay.

11 And I'll -- so I want to go through the different
12 methods that you used to detect the accounts. And was one
13 method or filter that you used related to the mail header?

14 A. Yes.

14:34:21 15 Q. And what is a mail header?

16 A. A mail header is a piece of information that your
17 e-mail program automatically puts into a hidden part at the
18 beginning of every e-mail that you send, and it identifies
19 what the software is that you're utilizing and the version
14:34:39 20 number of that software.

21 Q. Okay.

22 And what filter did you use related to the mail
23 header?

24 A. So I noticed that the bad guys were using two unusual
14:34:52 25 e-mail programs. I've written here, which one is called

Drake - Direct/Levine

1 Courier, with a version 3.50.00.09.1098. And the second one
2 was Group Wise Internet Agent 6.04 beta. These were unusual
3 in that no other customer of our entire service used these,
4 other than these two e-mail programs, and the majority of
14:35:17 5 what were being sent through these accounts came from one of
6 those two.

7 **Q.** Okay.

8 And do you see anyone not affiliated with this scheme
9 using those two e-mail headers?

14:35:28 10 **MR. O'SHEA:** Objection.

11 **MR. GOLDBERG:** Objection.

12 **THE COURT:** Sustained. One moment, sir. Next
13 question.

14 **MR. LEVINE:** Okay.

14:35:39 15 **Q.** When you were gathering these e-mails and incurring
16 these charges, one of the things you were doing was looking
17 at the content of the e-mails?

18 **A.** Initially, no, we don't keep copies of any customer
19 content, but we do keep the subject line and the center and
14:36:02 20 recipient of the e-mail. So I was looking at the subject
21 lines.

22 **Q.** And based on the subject lines, what were all these
23 e-mails from these various accounts about? What did they
24 have in common?

14:36:15 25 **A.** So they were about a few different topics.

Drake - Direct/Levine

1 One common thread was the perpetrators sending e-mails
2 that had the word second chance offer for item and something
3 to do with an eBay item or eBay payment invoice for item and
4 something to do with an eBay item.

14:36:51 5 MR. LEVINE: Just for us.

6 THE COURT: I can't hear you.

7 MR. LEVINE: I'm sorry. Can --

8 THE COURT: Are we still on 1321?

9 MR. LEVINE: Yes. Counsel for defense asked
14:36:59 10 if we could -- if we could look at it on the screen amongst
11 us.

12 MR. O'SHEA: Without the jury seeing it,
13 Judge, that's all we're trying to do, and I guess they tried
14 that and the jury got to see it.

14:37:10 15 THE COURT: All right. Go ahead.

16 MR. LEVINE: Okay.

17 BY MR. LEVINE:

18 **Q.** All right.

19 So you identified this unusual e-mail header and
14:37:22 20 the -- there were two unusual headers. One you said was
21 Courier and -- Courier with a long version number and one
22 Group Wise Internet Agent 6.0.4 beta; is that right?

23 **A.** Yes.

24 **Q.** Had you ever seen those e-mail address -- those
14:37:41 25 headers, those e-mail clients outside of this particular

Drake - Direct/Levine

1 context?

2 **A.** No, I specifically chose those because they were not
3 associated with anyone else, except for these people.

4 **Q.** Okay.

14:37:55 5 And was one of the e-mail filters you used related to
6 the subject line of the e-mails?

7 **A.** Yes.

8 **Q.** And can you explain what that e-mail filter was?

9 **A.** So if an e-mail came through that contained the words
14:38:11 10 "second chance offer for item" at the beginning of the
11 subject line, or the word "eBay payment invoice for item" at
12 the beginning of the subject line, I noticed that those also
13 were uniquely related to these scammers and weren't
14 something that any of my other customers were doing.

14:38:27 15 **Q.** Okay.

16 And did you also -- so you filtered, based on mail
17 header, on subject line, and did you also filter based on
18 account sign up information?

19 **A.** Yes.

14:38:44 20 **Q.** Okay. If we could bring up --

21 MR. LEVINE: Any objection to us bringing this
22 up as a demonstrative so we can explain what he --

23 MR. O'SHEA: Yes.

24 MR. LEVINE: Yes, you have an objection?

14:39:17 25 MR. O'SHEA: This is a portion --

Drake - Direct/Levine

1 THE COURT: Folks, if you're going to talk
2 privately, the Court Reporter doesn't know what's on the
3 record and what's not. So if you're going to talk amongst
4 yourselves, it needs to be private. Otherwise, you need to
14:39:32 5 include me.

6 MR. O'SHEA: Can I suggest we do it at side
7 bar, Judge?

8 THE COURT: If you're objecting to this being
9 shown, don't show it.

14:39:40 10 MR. O'SHEA: Okay. Let me talk to
11 Mr. Gallegos.

12 (Counsel conferring.)

13 MR. O'SHEA: Worked it out.

14 THE COURT: All right.

14:40:19 15 MR. LEVINE: Could we publish Exhibit 1321,
16 your Honor, please? The portion that's currently visible on
17 the screen.

18 THE COURT: Mr. Goldberg, any objection?

19 MR. GOLDBERG: No, your Honor.

14:40:32 20 THE COURT: Mr. O'Shea?

21 MR. O'SHEA: No objection.

22 BY MR. LEVINE:

23 Q. Okay.

24 So did you also filter, based on account sign up
14:40:43 25 information?

Drake - Direct/Levine

1 **A.** Yes.

2 **Q.** Okay.

3 And looking at this chart here, and it continues down
4 if necessary to help, will that help you explain how you
14:40:54 5 filter based on account sign up information?

6 **A.** Yes.

7 **Q.** Okay.

8 So looking at this chart, what accounts sign-in
9 information did you consider?

14:41:04 10 **A.** So we looked at the e-mail addresses that were being
11 chosen by -- we manually looked at all new accounts being
12 opened, and when we saw patterns we recognized, we would
13 flag the accounts. Some of the patterns we would look for
14 would be the letters ITP in the e-mail address. You can see
14:41:25 15 that ITP appears in all of these example e-mails or these
16 actual e-mails from our system.

17 We also look at the names people chose. So you'll
18 notice here that even though we have two different sign-ups
19 for Brian, they both have the same name so we know those
14:41:41 20 were probably the same person.

21 And we also look at the time zones the customer would
22 use. We have customers globally. We ask our customers to
23 choose what time zone they're in. So if the customers
24 happen to choose a similar time zone, each time we could
14:41:59 25 theorize they're related. But one of the most telling

Drake - Direct/Levine

1 methods of detection was our system asks the customers to
2 choose a secret question and an answer to that question,
3 just in case they forget their password. And a normal
4 customer would choose something like what was your first car
14:42:18 5 and then have an answer like a Ford Falcon or an American
6 car. But most of the fraudulent accounts would just put
7 completely stupid questions and answers in there.

8 So you can see examples here. We have a question of
9 T-E-S and an answer of Wesley or these other words that
14:42:36 10 don't make sense. But that's not the kind of thing that a
11 normal customer would ever put in those two boxes.

12 **Q.** Okay. And what was the significance of ITP in the
13 user name?

14 **A.** At that time, ITP was the brand that was being used by
14:42:57 15 the scammers for the --

16 MR. O'SHEA: Objection.

17 THE COURT: Overruled. Go ahead, sir.

18 THE WITNESS: The website they were directing
19 the victims to were using ITP as the brand name.

14:43:11 20 BY MR. LEVINE:

21 **Q.** Okay. And did you also manually flag customer
22 accounts that came to your attention as a result of credit
23 card charge back events?

24 **A.** Yes.

14:43:21 25 **Q.** Okay.

Drake - Direct/Levine

1 And did you collect the e-mails that were sent and
2 received by all those accounts that you referenced?

3 **A.** So at least initially, no. Our system doesn't record
4 those details, but later on, we decided to start looking at
14:43:42 5 what was actually going on inside the e-mails. So we did
6 start collecting them.

7 **Q.** Okay.

8 So when your filtering system identified these
9 e-mails, what would you do with them?

14:43:55 10 **A.** We forwarded them to our Gmail account.

11 **Q.** Okay.

12 Tell me about this Gmail account. How did you end up
13 forwarding to a Gmail account?

14 **A.** I set up a Gmail account in case anyone in the future
14:44:11 15 needed to look at the contents of these e-mails. My
16 motivation was to try and stop these people doing credit
17 card charge backs because it was costing a lot of money, and
18 I figured if I could get the information about the
19 activities to someone who could investigate, they could
14:44:25 20 hopefully shut them down and stop them causing me so much
21 money and stop the victims being caused so much grief.

22 **Q.** All right.

23 And at some point, did you get in touch with Special
24 Agent Lough, now Special Agent Diaz?

14:44:46 25 **A.** Yes.

Drake - Direct/Levine

1 Q. How did you end up getting in contact with her?

2 A. I don't remember the specifics. It was a long time
3 ago.

4 Q. Okay.

14:44:57 5 Did she contact you or you contacted her but somehow
6 you got connected?

7 A. So I contacted the Australian Federal Police and
8 others, including eBay and various others in an attempt to
9 stop these people, and somewhere the FBI were involved. I'm
14:45:15 10 not sure whether that was the result of me reaching out or
11 them looking for me.

12 Q. Okay.

13 And if you could just speak up a little louder in your
14 answer, pull the mike a little closer. I want to make sure
14:45:27 15 everyone can hear.

16 Handing the witness what has been previously marked
17 as, and referred to by Special Agent Diaz, this is
18 Government's Exhibit, CD Government's Exhibit 1320.

19 And have you had an opportunity to review Government's
14:45:51 20 Exhibit 1320 before taking the stand?

21 A. Yes.

22 Q. Okay.

23 And having had an opportunity to review Government's
24 Exhibit 1320, what does Government's Exhibit 1320 contain?

14:46:00 25 A. It contains the e-mails sent by my system to the Gmail

Drake - Direct/Levine

1 account I just mentioned.

2 Q. Okay.

3 And was Special Agent Diaz ultimately given access to
4 that Gmail account?

14:46:14 5 A. Yes.

6 Q. By you?

7 A. That's right, yes.

8 Q. Okay.

9 And does Exhibit 1320 contain fair and accurate copies
14:46:23 10 of the e-mails you filtered and provided to Special Agent
11 Diaz through the Gmail account?

12 A. Yes, it does.

13 Q. And roughly how many e-mails does Government's Exhibit
14 1320 contain?

14:46:33 15 A. It's tens of thousands. Roughly I think 19,000 or so.

16 Q. Okay.

17 (Counsel conferring.)

18 Q. Okay.

19 And I'm going to -- so, your Honor, I am showing,
14:47:25 20 publishing Exhibit 1328 in connection with having previously
21 discussed this exhibit and subsequent exhibits with counsel.

22 THE COURT: 1328? You can just identify it
23 and show it if you already know there's no objection.

24 MR. LEVINE: Thank you, your Honor.

25

Drake - Direct/Levine

1 BY MR. LEVINE:

2 **Q.** Okay.

3 So I'm going to also hand Mr. Drake the full e-mail
4 1328. So, Mr. Drake, what I'm showing on the screen is the
14:48:01 5 end of this e-mail chain. Can you just provide a little bit
6 of context? What is the context for the end of this e-mail
7 chain that's visible right now?

8 **A.** So we can see on the screen the response from the ITP
9 people back to the customer who is asking where his car is.

14:48:27 10 **Q.** And is the customer threatening to report the IT
11 people?

12 MR. O'SHEA: Objection.

13 THE COURT: Sustained.

14 **Q.** Okay.

14:48:36 15 Well, can you read the response from, that ends this
16 Read Notify e-mail?

17 **A.** ITP has written back to the victim of their fraud and
18 have written, "For reporting me, you should never mess with
19 people that can hurt you. But, never mind. I see that
14:48:55 20 you're a suborn mule and you will shortly be able to see
21 that God is Almighty. And God has your address. 9232 Wood
22 Stork Drive, DdR. So you can either start being real polite
23 or start packing. And since you are the 'I will report you'
24 kind, you can ask FBI. They will be able to confirm that
14:49:17 25 you are dealing with organized crime here."

Drake - Direct/Levine

1 Q. Okay. Thank you.

2 And let me -- let me ask you briefly, are most of your
3 customers like Read Notify criminals or is this unusual?

4 MR. GOLDBERG: Objection.

14:49:38 5 THE COURT: Sustained.

6 Q. What are the -- what are most of your -- how many
7 users do you have, by the way? How many customers do you
8 have approximately?

9 A. We have approximately a million customers.

14:49:46 10 Q. Okay.

11 And are most of them legitimate businesses?

12 A. Yes. So the majority of our customers --

13 MR. GOLDBERG: Objection.

14 THE COURT: Overruled. I'll allow you to
14:50:12 15 answer that.

16 THE WITNESS: Majority of our customers are
17 people who have legitimate reason to know about the
18 disposition of their e-mail. So it will be people who are
19 using it for sending invoice and need to know whether the
14:50:11 20 invoice has been opened and the community of victims of
21 romance scams. So if you think you're falling in love with
22 someone overseas, often they will use our service to write
23 an e-mail to the person overseas. And we are very good at
24 telling them they're not really who they think they are.
14:50:31 25 It's a huge problem. Number 1 way of females losing money

Drake - Direct/Levine

1 in our country. And it's a lot of people using our software
2 always as far as I can see for legitimate reasons.

3 **Q.** Okay.

4 Now, if we were to look at the header information for
14:50:51 5 this e-mail -- oh, I'm sorry. The formatting looks very
6 strange. Can you explain why that is?

7 **A.** So this is the hidden part of the e-mail that you
8 don't normally see. It's the byte that the e-mail systems
9 use to tell one another about things in your e-mail that
14:51:23 10 aren't actually part of the body of the e-mail.

11 **Q.** And does the coding in this header, does that help you
12 confirm that these e-mails were sent over Read Notify?

13 **A.** Yes.

14 **Q.** How does it do that?

14:51:38 15 **A.** So this -- three ways you can tell. The most obvious
16 one you can see here that the recipient has "dot
17 readnotify.com" on the bottom. Am I able to draw on this or
18 does it --

19 **Q.** Yes.

14:51:51 20 **A.** If you can see the arrow, you can see there's a -- is
21 that my arrow showing there? You can see it says "dot
22 readnotify.com" on the end of the recipient. So this
23 indicates this is a mail received by my server before we've
24 done the processing to take that off. Also at the top here
14:52:09 25 is information that only my server adds for sign internal

Drake - Direct/Levine

1 purposes.

2 **Q.** Okay.

3 So you said that was before your server takes that
4 off. So once the recipient receives it, they will not see
14:52:22 5 that Read Notify information there?

6 **A.** That's right. This is the e-mail literally as it was
7 received from the sender before my system's made any changes
8 to it.

9 **Q.** Okay.

14:52:36 10 And ignoring the strange formatting and coding, is the
11 text of all -- of all these e-mails, all the true and
12 accurate original texts as the -- as it was sent and as it
13 would be received?

14 **A.** Well technically, it's changed from sending before it
14:52:57 15 gets to me. You can see that the intermediate service put
16 their own identity in here with the received headers. And
17 then, of course, my system will add the tracking, which
18 changes it from when it's received, but this is the format
19 that's arrived to my server after it's been sent by the
14:53:12 20 sender in its original entirety.

21 **Q.** All right.

22 So can you use walk us through what -- taking a look
23 at this, what is the -- we see a "from." Who is the from?

24 **A.** This is the -- there's two parts here. You'll see
14:53:41 25 there's a part here, an apostrophe. So that's the name of

Drake - Direct/Levine

1 the sender. The person has no name. So they put their
2 e-mail address as the name. So the e-mail comes second and
3 so that's the person who sent it, the from.

14:53:55

4 **Q.** I want to try to walk from the top of the e-mail
5 towards the bottom.

6 So what we're seeing here is the header information.
7 So at the have he top, there's a "from" there as well. And
8 it says, "Mailto Blackhole devnull@srve.com"?

9 **A.** Okay.

14:54:08

10 So my system took an original e-mail, and then it sent
11 it as an e-mail to the Gmail account that I was talking
12 about.

14:54:27

13 So what you've printed here is an e-mail that inside
14 it contains another e-mail. So you'll see here the e-mail I
15 sent you in its original format, complete with all the
16 headers. The stuff at the top is what my system identifies
17 itself as when it sends this to that Gmail account.

18 **Q.** Okay.

14:54:42

19 So does that mean that everything above the line that
20 we see there relates to you forwarding all these to your
21 Gmail account?

22 **A.** That's right. It's unrelated to this e-mail itself,
23 other than that's the moment in time that my system sent it
24 to you.

14:54:52

25 **Q.** Got it. Okay.

Drake - Direct/Levine

1 So then below the line, we have a -- what is that
2 line, the UTC?

3 **A.** That's my system putting my system's time above the
4 message it's sending to you. And sometimes computers use
14:55:10 5 different time zones. So I put it in explicitly with UTC so
6 everyone knows what time this really was, and not plus or
7 minus some amount of hours, depending on time zone.

8 **Q.** What is UTC?

9 **A.** Universal Time Coordinate, I think. It's -- Greenwich
14:55:29 10 mean time, the base time all computers use themselves.

11 **Q.** Okay.

12 So then we have a line that says, "X-Arg1." What is
13 that line?

14 **A.** So the older lines that begin with X-Arg1, we use a
14:55:43 15 format called SMTP, which stands for Simple Mail Transfer
16 Protocol. And in that format, computers will connect to one
17 another. And then they'll make a request. And typically,
18 that will be, "Hello. My e-mail address is impala63ss1.com,
19 and I want to send a message to
14:56:06 20 Craig.McKeever@comcast.net.readnotify.com," and the
21 recipient machine will agree that's okay and ask for the
22 message.

23 So that's not part of the e-mail headers but are
24 included here because my system knew that at the time and
14:56:16 25 thought you might be interested in knowing that.

Drake - Direct/Levine

1 So X-Arg1 is just an internal switch that my system
2 uses to identify what kind of message coming in. X-Arg2 is
3 what's called the SMTP mailed from address. That's the
4 sender e-mail address.

14:56:36 5 X-Arg3 is the RP address that was connected -- they
6 connected to my mail server from. So their mail server is
7 connected to my mail server, in this instance using the IP
8 address 76.13.13.45.

9 And then X-Arg4, and if there's anymore XR's after 4,
14:56:53 10 the one or more recipients that have been addressed in the
11 e-mail it's about to follow. And then the message
12 separated, the last one there, just so you know, mine are
13 finished and the e-mail then begins, the content.

14 **Q.** The e-mail officially begins after the message
14:57:09 15 separated the lines MSGSEP?

16 **A.** Yes, where the -- all e-mail starts with the word
17 "from" and a space. So that's where the actual e-mail
18 begins.

19 **Q.** Okay.

14:57:19 20 So then the next line, you see it's from who? What
21 e-mail address?

22 **A.** So the "from" here is going to be what the sender
23 identified, or the sender himself identified themselves as
24 when it connected in order to send an e-mail.

14:57:39 25 **Q.** Okay.

Drake - Direct/Levine

1 And that's -- what is that e-mail address, so we're
2 looking --

3 **A.** Impala63SS@ymail.com.

4 **Q.** Okay.

14:57:52 5 Okay.

6 And so then going back to what we had before, what is
7 the e-mail address that's sending this e-mail and who are
8 they sending it to?

9 **A.** So that XArg -- so the "from" in this instance matches
14:58:26 10 what we saw above. E-mail is kind of funny. You can put
11 anything you like in the from area of an e-mail and it
12 doesn't have anything to do with who you really are but in
13 this case, it does match, which is why you see e-mails at
14 the beginning as well as in the "from."

14:58:42 15 So this e-mail is sent from this e-mail address,
16 impala63SS@ymail.com. And the recipient is going to be
17 craig.mckeever@comcast.net.readnotify.com, which is why it
18 comes to my server before we strip that off and send it to
19 Craig.

14:59:03 20 THE COURT: Mr. Levine, I think we need to
21 take an afternoon break.

22 MR. LEVINE: Okay.

23 THE COURT: Is this a good place or you want
24 to do a couple followups?

14:59:13 25 MR. LEVINE: I -- just one question.

Drake - Direct/Levine

1 THE COURT: Go right ahead.

2 Q. Is Government's Exhibit 1328, the one you're looking
3 here, is this one of the e-mails that you provided to
4 Special Agent Diaz via the Gmail account?

14:59:26 5 A. Yes. You can see it's matched my tag here with the
6 name I mentioned before of the e-mail program they used.

7 MR. LEVINE: Okay. Let's -- we can proceed to
8 a recess if you'd like, your Honor.

9 THE COURT: Folks, we will take our afternoon
14:59:41 10 recess. Please remember the admonition.

11 All rise for the jury.

12 (Thereupon, a recess was taken.)

13 THE COURT: Mr. Levine, you may continue, sir.

14 MR. LEVINE: Thank you, your Honor.

15:24:09 15 BY MR. LEVINE:

16 Q. Mr. Drake, a question arose, came up in my mind while
17 we were having that break, which is Microsoft Outlook has a
18 read receipt feature. And I sometimes get e-mails where the
19 sender wants me to confirm I received the e-mail.

15:24:23 20 How is that different from your feature, your server?

21 A. Our system allows our users to decide whether or not
22 the recipient will be asked that question, and irrespective
23 of whether the recipient sees it and whatever they might
24 answer, our system always reports when the e-mail has been
15:24:44 25 opened and information about the opening.

Drake - Direct/Levine

1 Q. Okay. Thank you.

2 But it's similar in the sense that it's a receipt for
3 someone who reads or someone who received an e-mail?

4 A. Yes.

15:24:57 5 Q. Okay.

6 So I'd like to now bring up Government's Exhibit 1329.
7 And first, I want to look at this header information. I cut
8 off some of it, unfortunately, but from that header
9 information, can you tell is this one of the e-mails that
10 you provided Special Agent Diaz via the Gmail account?

11 A. Yes, it is.

12 Q. Okay.

13 And what I want to do now, I want -- start at the
14 bottom of the chain. This is a five-page e-mail, and we're
15 just going to look at the e-mails and every other e-mail.
16 So we're going to start with -- start with this e-mail right
17 here.

18 MR. LEVINE: We're experiencing minor
19 technical difficulties.

15:26:36 20 THE COURT: Have anything to do with the arrow
21 being on?

22 MR. LEVINE: Shouldn't.

23 THE COURT: Okay. Okay.

24 Q. Mr. Drake, could you read this e-mail right here?

15:27:15 25 A. "This is," being the end of the e-mail that's, all of

Drake - Direct/Levine

1 this part of the conversation, "just to get a perfect idea
2 of how this vehicle looks like and its awesome condition, I
3 have uploaded some new pics on Kodak. Feel free to check
4 them out."

15:27:31

5 Q. Okay.

6 Now, by the way, those equal signs we see there, would
7 the recipient of this e-mail see those equal signs?

15:27:48

8 A. No, say that's -- multi-part flowed format. That just
9 indicates to the malprogram that the line actually continues
10 and the equals would be removed.

11 Q. Okay.

12 And that thing you see at the bottom, is that what we
13 call a link?

14 A. That's a web link, yes.

15:27:57

15 Q. And what is a web link?

16 A. That's something that a recipient can click on which
17 will open the Internet browser and download whatever it's
18 pointing to.

19 Q. Okay.

15:28:08

20 Now, we're going to skip to the next one here, where
21 -- from trucking200@ymail.com. So we're looking at every
22 other e-mail in this conversation.

23 Could you read this e-mail?

15:28:27

24 A. "Yes, it's all steel. Absolutely nothing wrong with
25 the car. Everything in perfect running order. Engine runs

Drake - Direct/Levine

1 great, too. I'm selling because I need the money real fast
2 and I'm not home to take care of it any better. So it's got
3 to go over the Internet. That's why the low price. Thing
4 is I was counting on this sale a couple weeks ago when I had
15:28:46 5 the deal with the buyer who backed out because of loan
6 problems. So if you have the money, I would appreciate you
7 buying it ASAP. Thanks."

8 **Q.** Okay.

9 And again, the equal signs we see here, the
15:29:01 10 recipient's e-mail would not see those equal signs?

11 **A.** No.

12 **Q.** Okay. Let's read -- if you wouldn't mind, please read
13 this e-mail?

14 **A.** "No, I haven't made the modifications myself. I've
15:29:15 15 bought it the way it is. Let me know when you have sent the
16 money to eBay and please e-mail me your shipping address so
17 I can take care of it ASAP."

18 **Q.** And if you would please read this e-mail.

19 **A.** "Well I am still waiting for eBay to confirm. After I
15:29:33 20 am satisfied that they hold the money, I will give you all
21 the info. By the way, what's your shipping address?" BTW
22 means by the way.

23 **Q.** Okay. If you will read this e-mail, please.

24 **A.** "I just got off live help with eBay. They alerted me
15:29:56 25 that they sent the money back to you by mistake. You should

Drake - Direct/Levine

1 get there and talk to them, too."

2 Q. Okay.

3 A. "Just got off chatting with eBay. They did return the
4 money to your account but it may take 24 business hours to
15:30:17 5 post. I have asked them to assign a new agent and they have
6 done so. And you are also getting a \$200 discount from
7 eBay. So I guess it kind of sucks having to wait like that,
8 but as soon as you get the refund, please send it again so
9 we don't waste any more time. Thanks."

15:30:39 10 Q. The trucking200 e-mail would go right here.

11 A. Again, he said "do what? Why did you cancel your
12 payment? That's what eBay told me."

13 Q. Okay. And then the last e-mail which you can see
14 starts here and the header information and the content
15:31:01 15 begins here.

16 A. "1. Why is your family hurting? Are you beating your
17 wife and children? 2. You are being delusional. The point
18 of scamming you is to get your money. Therefore, the right
19 thing is to keep it. Why have you contacted the
15:31:18 20 authorities? Not that I care but I think you're trying to
21 fuck with me here. And my advice to you is not to fuck with
22 people that can hurt you. Apologize for that. That's all I
23 ask. Last and most importantly, you should thank me as I
24 have saved your ass in a number of ways. Such a car is
15:31:36 25 completely useless. Therefore, a waste of your and your

Drake - Direct/Levine

1 family's money. So at least you ended up spending less than
2 half of what you would have lost on a real car. It's also
3 unsafe. What if you and your family are involved in an
4 accident in such a vehicle? I think hospitalization would
15:31:51 5 hurt them more than you beating them. I await your
6 apologies. And thanks. Cheers."

7 **Q.** All right.

8 Finally, if we could please bring up Exhibit 1330 and
9 let's first start looking at the header information there.

15:32:23 10 Looking at the header information, can you tell
11 whether this is one of the e-mails you provided to Special
12 Agent Diaz via the Gmail mailbox that you identified?

13 **A.** Yes, it is.

14 **Q.** Okay. So now can you -- all right. If you'd please
15:32:56 15 read this e-mail to the jury. Thank you very much.

16 **A.** "Hello, Maria. Sorry for getting into your lives.
17 I'll get straight to the point as it's kind of late now. I
18 wanted to sell my car and Mike replied to an ad of mine.
19 Then he started using harsh language, offended me, and
15:33:13 20 although I'm man of understanding, I ended up not tolerating
21 his shit. Being bright with computers, I thought of
22 teaching him a lesson and wiping his files, e-mail accounts
23 and other accounts he may have with other websites. This is
24 what I wanted to do at first, but hey, I'm not irrational.
15:33:29 25 I thought it up for a moment. I could have done a lot of

Drake - Direct/Levine

1 harm to other innocent people, and I started investigating
2 more about him and what kind of man he is. I went from the
3 idea that he's a fucking moron, and the way he is treating
4 you as a wife confirmed this to me.

15:33:45 5 "I don't want to do any harm to you, just to the
6 moron, Mike, who treated me with very big disrespect, and I
7 want you to find out something about his love affairs and
8 about what he does when he's out there in the freedom for
9 hours by himself or when you think he's at work. Check out
15:34:04 10 those e-mails between him and Lana O'Brien,
11 lanarossman@AOL.com, at the end of this. It starts out
12 easily then gets more passionate. If you don't believe me,
13 then log into his Yahoo account. User name,
14 ELMikey7@yahoo.com, and password 2559750, and search through
15:34:28 15 the messages in the sent folder. You will find those there.
16 Check the messages from the inbox as well. There were some
17 there but not as passionate as those from the sent folder.
18 He took care to delete the incriminating -- the ones
19 incriminating him maybe.

15:34:43 20 "Oh, and you can even ask Laura. You may be wondering
21 why I'm doing this. I could have erased all the data in
22 your eBay account as well as my seventeen, but seeing what a
23 jerk this husband of yours is and that he's having nothing
24 to do with you, and this having nothing to do with you,
15:35:04 25 moreover, he's a jerk to you, too. I change my mind. Yours

Drake - Direct/Levine

1 Mr. X. Here are e-mails between Mike and Lana, starting
2 2007 up to 2010."

3 Q. Okay.

4 And we -- we will not -- we will not read all the
15:35:20 5 e-mails between Mike and Lana starting in 2007 up to 2010.

6 In total, roughly, how much did the Bayrob Group cost
7 Read Notify?

8 A. So there was about \$2,000 worth of charge backs for
9 the credit cards and hundreds of hours of wasted time
15:35:49 10 dealing with the charge backs. And reputation damage that
11 was done, hard to put a total cost on it, but it would be in
12 the tens of thousands.

13 Q. Okay. Okay.

14 MR. LEVINE: Thank you, your Honor. The
15:36:08 15 Government has no further questions for this witness.

16 THE COURT: Cross-examination, Mr. Goldberg.

17 MR. GOLDBERG: Thank you, your Honor.

18 The Defense waives cross-examination of this witness.

19 THE COURT: And Mr. O'Shea?

15:36:18 20 MR. O'SHEA: Just a couple quick questions.

21 THE COURT: Certainly.

22

23

24

25

Drake - Cross/O'Shea

1 CROSS-EXAMINATION OF CHRISTOPHER DRAKE

2 BY MR. O'SHEA:

3 **Q.** Thank you for crossing the pond there, Mr. Drake. I
4 appreciate it.

15:36:30 5 How many hours were you on the plane?

6 **A.** 26.

7 **Q.** Wow.

8 **A.** Three different planes.

9 **Q.** Okay.

15:36:36 10 Now, a couple quick questions, sir. And they go back
11 to just this business before about Outlook and how Outlook
12 has a function or a program similar to what we're talking
13 about with Read Notify.

14 Are you aware that Outlook gives you a choice when you
15:36:52 15 send an e-mail to both, say it's read as well as delivered,
16 there are two choices that you get from Outlook. Are you
17 aware of that?

18 **A.** Yes, sir. One is called MDN or Message Disposition
19 Notification, and the other one is return receipt.

15:37:08 20 **Q.** Okay.

21 **A.** Different thing.

22 **Q.** One of them basically tells you that the person
23 actually opened up and read the e-mail as opposed to the
24 other one which says I know it got there?

15:37:18 25 **A.** Yes, one for delivery, one for opening.

Drake - Cross/O'Shea

1 Q. Okay.

2 Does Read Notify do something similar to that as well
3 or is it just always when it's been read?

4 A. It's -- we always do both.

15:37:30 5 Q. Okay.

6 And you can -- can you tell that from the header?

7 A. No.

8 Q. Okay. Fair enough. You have been asked --

9 THE COURT: I'm sorry, sir?

15:37:41 10 THE WITNESS: We always do. It's no way to

11 tell from the header because we always do both.

12 Q. Okay. But, does the person who gets the e-mail have a
13 choice of declining to send back a read receipt or a --
14 strike that.

15:37:55 15 The person, when you use Outlook, has the ability to
16 decline sending back a read receipt, am I right about that?

17 A. You mean the recipient?

18 Q. Yes.

19 A. Recipients sometimes are given that option, yes.

15:38:11 20 Q. Okay. But they don't have that option whether it
21 comes to -- whether or not, whether or not the e-mail was
22 delivered as opposed to read, right?

23 You get it back, using that Outlook feature, you'll
24 get notification it's been delivered but -- and the

15:38:25 25 recipient has no control over that; whereas, the recipient

Drake - Cross/O'Shea

1 gets to decide whether or not they click on what is
2 essentially a certified mail receipt, am I right?

3 **A.** That's right.

4 **Q.** With Outlook. I'm limiting it to Outlook. Am I right
15:38:39 5 about that?

6 **A.** That's right.

7 **Q.** And just to translate that over to Read Notify, does
8 Read Notify have such a feature that the recipient gets to
9 decide whether or not the person that sent the e-mail is
15:38:56 10 notified, that they have actually opened and read it?

11 **A.** All senders get to choose whether the recipients see
12 that. It's up to what selection the person made when they
13 open an account with our service.

14 **Q.** Does the recipient even know that Read Notify is being
15:39:13 15 used?

16 **A.** It's like I said. It's if the sender chooses to let
17 them know, yeah; otherwise, no.

18 **Q.** If the sender chooses not to let them know, then they
19 don't know, right?

15:39:24 20 **A.** That's right.

21 **Q.** All right.

22 Now you were asked a lot of questions on direct
23 examination and the term that was used, Mr. Drake, was the
24 Bayrob Group. Remember that?

15:39:36 25 **A.** I don't specifically remember that, no. I knew them

Drake - Cross/O'Shea

1 as ITP.

2 Q. ITP. All right.

3 Who told you or introduced you to the term Bayrob
4 Group? Who did that?

15:39:50 5 A. I don't remember.

6 Q. Okay.

7 It wasn't you, right? You didn't deem this group the
8 Bayrob Group, am I right?

9 A. No.

15:39:58 10 Q. Okay.

11 But prior to you coming to America and sitting on this
12 witness stand, somebody has told you that we're referring to
13 this group as the Bayrob Group, am I right?

14 A. Probably, yes. I've heard the name, yes.

15:40:12 15 Q. And you were asked questions about this e-mail coming
16 from the Bayrob Group, but we read some e-mails that were,
17 you know, insulting ones that said some mean things to some
18 folks, it was implied, sir, that those e-mails came from the
19 Bayrob Group, but you have no idea, right?

15:40:32 20 A. Look, I apologize. I don't remember Bayrob being
21 mentioned. Sorry.

22 Q. Okay.

23 But, you don't know -- let me ask another way. You
24 have no idea as you sit here now who sent those insulting
15:40:44 25 comments that you got to read, am I right about that?

Drake - Redirect

1 **A.** That's right.

2 MR. O'SHEA: Nothing further. Thank you, sir.

3 THE COURT: Based on those questions.

4 MR. LEVINE: Yes, I have just a couple

15:41:02 5 follow-up.

6 REDIRECT EXAMINATION OF CHRISTOPHER DRAKE

7 BY MR. LEVINE:

8 **Q.** You just testified you have no idea who sent those
9 insulting comments by which -- by which you mean you don't

15:41:14 10 know who's behind the keyboard?

11 **A.** That's correct.

12 **Q.** Okay.

13 But you testified in great detail how you identified
14 this universe of documents related to this particular group,
15:41:26 15 correct?

16 **A.** That's right.

17 **Q.** All right.

18 And what did you refer to this group as prior to
19 hearing the term Bayrob Group?

15:41:35 20 **A.** We called them ITP. Like I said, that was the brand
21 they were using when they first started doing charge backs
22 on our service and you'll see the exhibit when we first saw
23 that, like all different names they used. I wouldn't know
24 if one of those was their real name or not.

15:41:50 25 **Q.** Okay.

Drake - Redirect

1 And all of the -- all of the 19,000 approximate
2 e-mails on this CD, they are all e-mails that met the filter
3 criteria that you described earlier?

4 **A.** Yes.

15:42:02 5 **Q.** All right.

6 This -- all the e-mails on the CD, are they all
7 e-mails as of the time they hit your server?

8 **A.** Yes. So they would come in my server and my server
9 would send them immediately when they match my filters to
15:42:23 10 the Gmail account.

11 **Q.** So is any of the read information that would be sent
12 to the recipient of that e-mail, is any of that read
13 information in any of these e-mails?

14 **A.** No.

15:42:35 15 **Q.** Okay.

16 MR. LEVINE: No further questions, your Honor.

17 MR. O'SHEA: One moment, please.

18 THE COURT: Recross, Mr. Goldberg?

19 MR. GOLDBERG: Very briefly.

15:42:50 20

21

22

23

24

25

Drake - Recross/Goldberg

1 RECROSS-EXAMINATION OF CHRISTOPHER DRAKE

2 BY MR. GOLDBERG:

3 **Q.** The question for you is when a recipient receives an
4 e-mail through your server, you've testified that a -- there
15:43:06 5 is an automatic notification to the sender that it's been
6 received?

7 **A.** Yes. Well, that it's being rendered for display on
8 the recipient's machine.

9 **Q.** And then when it's opened, there's another message
15:43:23 10 that goes to the sender that it's been opened and read?

11 **A.** Like I say, our system records the delivery, and it's
12 available to the sender, but that's not a notice they get.
13 They can just look that up if they're interested later
14 unless it's a bounce back. So if you send an e-mail and it
15:43:38 15 doesn't go through, we do tell you it didn't go through and
16 that's different from the receipt we do send when it's
17 opened.

18 **Q.** Okay.

19 And you indicated that the amount of time each page
15:43:48 20 was looked at or was displayed on the monitor of the
21 receiver is also recorded on your server?

22 **A.** Depends -- so if you're opening an attachment that was
23 on the e-mail, depending on your software using for the
24 attachment, then yes.

15:44:03 25 **Q.** And this is something the recipient would not be aware

Drake - Recross/Goldberg

1 of, correct?

2 **A.** Unless the sender has -- if the sender has chosen to
3 hide that from them, yes.

4 **Q.** So assuming the sender doesn't tell the recipient
15:44:17 5 this, you -- your system is able to access information from
6 the recipient's system and send that back to your server
7 without their knowledge, correct?

8 **A.** Yes.

9 **Q.** And that includes when the e-mail was opened, when
15:44:40 10 the -- when the attachments were opened and how long the
11 attachments were looked at, correct?

12 **A.** Yes.

13 **Q.** What else?

14 **A.** The IP address that was being used, the approximate
15:44:53 15 geolocation of that IP address and the software -- the
16 browsing software you're using. The same things any web
17 browser sends to every website that you access.

18 **Q.** And this is all otherwise private information that
19 your system's gathering without the recipient knowing?

15:45:11 20 **MR. LEVINE:** Objection.

21 **THE COURT:** Overruled. Is that true, sir?

22 **THE WITNESS:** I wouldn't class it as private
23 because everything you do on the Internet sends the exact
24 same information to the server. That's how the Internet
15:45:23 25 works.

Drake - Recross/Goldberg

1 Q. Okay.

2 Well, would an average user know that their
3 geolocation and the time of their -- amount of time they
4 spent viewing an attachment would be sent back through the
15:45:35 5 Internet to the sender?

6 MR. LEVINE: Objection.

7 THE COURT: Do you understand the question,
8 sir?

9 THE WITNESS: Whether someone's average. And
15:45:45 10 I'm not an average user. So I automatically know this. So
11 I don't know how many people would --

12 THE COURT: Objection sustained.

13 BY MR. GOLDBERG:

14 Q. Okay.

15:45:52 15 So you're saying this is something that people should
16 know otherwise, that this information is going -- is
17 available and goes back through the -- back to the server if
18 it's configured in that way?

19 A. As of today, I think most people, it's kind of common
15:46:12 20 knowledge this happens all the time, everything is being
21 tracked. Back in the beginning of this, it was probably not
22 as much common knowledge.

23 Q. Okay. Thank you very much.

24 MR. O'SHEA: Sorry. Nothing based on that,
15:46:29 25 Judge.

Drake - Recross/Goldberg

1 MR. LEVINE: Can I ask a follow-up?

2 No further questions, your Honor.

3 THE COURT: You may step down, sir. Safe
4 travels.

15:46:42 5 THE WITNESS: Thank you.

6 Mr. Levine, it's my understanding that you have a
7 stipulation.

8 MR. LEVINE: Yes, I think that's right, your
9 Honor.

15:46:54 10 I believe we have a stipulation between the parties as
11 to the accuracy of all the Romanian translations; that is,
12 the translations from English -- from Romanian into English
13 with one correction that I will make on the record. Okay?

14 So the correct correction -- the one correction which
15:47:34 15 was provided to me by the translator, who is here and
16 prepared to testify, is to Exhibit 426 and Exhibit 1084.
17 Both are the same communication, but I believe they're from
18 two different devices, which is why they're two separate
19 exhibits. So that's Exhibit 426 and Exhibit 1084.

15:48:04 20 In both instances, the communication is a one-sentence
21 communication. And the translation currently reads as,
22 "What should can I do, comma? I don't have the IP question
23 mark."

24 MR. O'SHEA: Exhibit 426? I'm sorry, Judge.
15:48:26 25 And the other Exhibit?

Drake - Recross/Goldberg

1 THE COURT: 1084.

2 MR. O'SHEA: 1084, and let me just quickly
3 look at them, Judge, to make sure. Just because we're
4 stipulating to accurate translation does not mean I agree
15:48:43 5 that the jury should hear it. That's -- I'm sorry.

6 THE COURT: I think it's just one sentence
7 that I --

8 MR. LEVINE: Correct.

9 THE COURT: I don't think it's going to be
15:48:53 10 very understandable without context, am I right, Mr. Levine?

11 MR. LEVINE: You're exactly right, your Honor.

12 THE COURT: All right.

13 So, "What should could I do, comma? I don't have the
14 IP question mark."

15:49:08 15 MR. LEVINE: Yes. That sentence should be,
16 "What update can I do, comma? I don't have the IP question
17 mark." And, in fact, if you look at the --

18 THE COURT: Don't go any further.

19 MR. LEVINE: Okay.

15:49:21 20 THE COURT: Don't go any further.

21 Mr. Goldberg, are you in fact stipulating to this
22 translation with that correction?

23 MR. GOLDBERG: We are, your Honor.

24 THE COURT: Mr. O'Shea?

15:49:38 25 MR. O'SHEA: We're stipulating to the

Drake - Recross/Goldberg

1 translation. That's it.

2 THE COURT: Correct.

3 MR. O'SHEA: Understood. Yes.

4 THE COURT: Correct. Not admissibility.

15:49:47 5 MR. O'SHEA: Yes, or showability I guess.

6 THE COURT: Right.

7 MR. LEVINE: I want to make sure for the
8 record that we're stipulating to all of the Romanian to
9 English translations, not just this one or two that I made,
10 correct?

11 THE COURT: Correct.

12 MR. O'SHEA: Thank you. So stipulated.

13 MR. GOLDBERG: That's correct, your Honor.

14 THE COURT: Ladies and gentlemen, a
15 stipulation is a fact agreed to by and between the parties.
16 And just to make it a little simpler, in other words, the
17 Government does not have to call as a witness the actual
18 translator. They are stipulating to the translation.

19 MR. LEVINE: Thank you, your Honor.

15:50:29 20 If you will pardon us for one moment.

21 THE COURT: Sure.

22 (Counsel conferring.)

23 MR. LEVINE: Your Honor, could we have a quick
24 bench conference?

15:50:46 25 THE COURT: Sure.

Drake - Recross/Goldberg

1 (The following proceedings were held at side bar:)

2 THE COURT: I knew it couldn't be simple. On
3 or off?

4 MR. GOLDBERG: I think it's purely on
15:51:07 5 scheduling.

6 (Discussion held off the record.)

7 MR. LEVINE: Okay. The United States would
8 like to call its next witness, Liam Omurchu.

9 THE COURT: Please step up to the podium, sir.
15:53:59 10 And please raise your right hand.

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Omurchu - Direct/Levine

1 LIAM OMURCHU,
2 of lawful age, a witness called by the GOVERNMENT,
3 being first duly sworn, was examined
4 and testified as follows:

15:54:20 5 DIRECT EXAMINATION OF LIAM OMURCHU

6 BY MR. LEVINE:

7 Q. Okay.

8 Could you please state and spell your name for the
9 record?

15:54:26 10 A. Sure. My name is Liam Omurchu. First name Liam,
11 L-I-A-M, last name, O-M-U-R-C-H-U.

12 Q. Okay.

13 Could I ask you to move the microphone a little closer
14 to you. And if you can speak a little louder. I noticed
15:54:44 15 you have a slight accent. Did you also travel from far away
16 to be here today?

17 A. I did. I'm from Ireland originally but traveled from
18 Los Angeles.

19 Q. Not quite as bad as Ireland. All right.

15:54:56 20 Mr. Omurchu, what do you do?

21 A. I work for Symantec, and I analyze software.

22 Q. All right. So what is your title?

23 A. My title is Director With Security Response.

24 Q. What is Symantec?

15:55:13 25 A. Symantec is a company that makes security software to

Omurchu - Direct/Levine

1 protect your computer, we make all sorts of different
2 products that you can use in your computer to protect you
3 from attacks.

4 **Q.** Okay.

15:55:28 5 So what types of products does Symantec make that
6 could protect your computer?

7 **A.** One of our main products is an antivirus product
8 called Symantec AntiVirus and also a product called Norton
9 AntiVirus that you install on your computer and it protects
10 you from viruses.

11 **Q.** Okay.

12 And do you have other products that protect your
13 computer from attackers?

14 **A.** Yes, we do. Symantec makes over 100 different
15:56:01 15 products and we protect you from network attacks. We can
16 restore files on your computer, make backups of files on
17 your computer, stop spam, lots of different things.

18 **Q.** Okay.

19 And you said you are a director at Symantec?

15:56:20 20 **A.** That's right.

21 **Q.** What department do you direct?

22 **A.** I work in the department called Security Response.

23 **Q.** All right.

24 What does Symantec's Security Response department do?

15:56:33 25 **A.** So what we do is we respond to security incidents. If

Omurchu - Direct/Levine

1 there is a virus that has been released by a virus author,
2 we pick it up, we analyze it, and we understand, try to
3 understand what it is that it does, and then we ship
4 protection to computers all over the world to make sure that
15:56:53 5 that virus cannot harm that computer.

6 Q. Okay.

7 And as a member of the Security Response Department,
8 were you involved in a Symantec investigation into the
9 Bayrob Malware and the Bayrob Group?

15:57:07 10 A. Yes, I was.

11 Q. Okay. I want to talk to you about that. But first I
12 want to briefly go through your background.

13 So can you tell us your educational background?

14 A. Sure. I went to study computer science in University
15:57:22 15 College Dublin in Ireland, and I have a bachelor of science
16 degree, specializing in computer science.

17 Q. Okay. So that's a BS in computer science?

18 A. That's correct.

19 Q. And prior to working with Symantec, did you work for a
15:57:35 20 company called TO Media?

21 A. I did.

22 Q. What was TO Media?

23 A. TO Media was a company with a startup company that was
24 trying to make advertisements appear on web pages before the
15:57:52 25 likes of Google and double clicked that.

Omurchu - Direct/Levine

1 Q. Okay.

2 And what do you do for TO Media?

3 A. I was writing JavaScript codes. I was a developer,
4 and I was writing code to make the advertisements appear on
15:58:06 5 the web pages.

6 Q. So does that mean you were actually a programmer?

7 A. I was a programmer, yes.

8 Q. And after working for TO Media, did you move to a
9 company called Brite-Mail?

15:58:17 10 A. I did.

11 Q. And what was Brite-Mail?

12 A. Brite-Mail is an anti-spam company. They were an
13 anti-spam company. What they do is they filter e-mail to
14 check, to block unwanted e-mail. So my role there was to
15:58:36 15 examine e-mail that was being sent to determine if it was
16 de-legitimate or if it was, you know, some sort of a scam or
17 spam, and if it was, I was to block that e-mail.

18 Q. And you used the term "spam." What do you mean when
19 you say spam?

15:58:52 20 A. Spam is unwanted e-mail. So unsolicited e-mail,
21 e-mail that you don't -- you haven't requested and it comes
22 to you knowing or often some sort of scam or advertisement
23 that you're not interested in.

24 Q. Okay.

15:59:10 25 And earlier, you used another term, JavaScript.

Omurchu - Direct/Levine

1 What's JavaScript?

2 **A.** JavaScript is a language that you can use to write web
3 pages in and to -- it's a programming language, and you use
4 that to write -- you use that to write web pages and make
15:59:34 5 web pages interactive.

6 **Q.** And you knew how to program in JavaScript?

7 **A.** Yes.

8 **Q.** And with Brite-Mail, what was your particular role?
9 What did you do?

15:59:43 10 **A.** In Brite-Mail, I was an anti-spam technician, which
11 was understanding e-mail, looking at the internals of each
12 e-mail that was being sent and to understand if it was
13 likely to have been unsolicited. And if it was unsolicited,
14 I would write code that would stop that e-mail from being
16:00:06 15 sent to any more recipients.

16 **Q.** Okay. And what happened to Brite-Mail?

17 **A.** Brite-Mail was acquired by Symantec.

18 **Q.** Symantec, is that the company you currently work for?

19 **A.** That's right.

16:00:16 20 **Q.** When was Brite-Mail acquired by Symantec?

21 **A.** In 2004.

22 **Q.** And is that when you moved over to Symantec?

23 **A.** That's correct.

24 **Q.** So you've been at Symantec for 14 years now?

16:00:29 25 **A.** Yes.

Omurchu - Direct/Levine

1 Q. 15?

2 A. 15 years now, yeah.

3 Q. So when you began at Symantec, what was your role?

4 A. When I began at Symantec, my role was to analyze
16:00:42 5 viruses, yeah, to analyze viruses, to monitor activity
6 online, online activity for malicious code, and to analyze
7 that malicious code.

8 Q. And when you started at Symantec, where were you
9 located geographically?

16:01:02 10 A. Dublin in Ireland.

11 Q. And were you a reverse engineer?

12 A. Yes, I was a reverse engineer, and what a reverse
13 engineer means is that a normal engineer builds code and a
14 reverse engineer takes that built code and deconstructs it
16:01:19 15 to understand the purpose of that code.

16 Q. Why would you need to do that?

17 A. Well, for many different reasons. The main reason I
18 was doing it was to understand why the code was written and
19 what was the purpose of the code. So mostly, I was looking
16:01:37 20 at malicious code, and I would like at the malicious code,
21 and then I would try to break it down to understand what
22 exactly the code was trying to do, what was the purpose, why
23 did it exist, who had written it, why had they written it.

24 So, for example, a malicious piece of code might be
16:01:57 25 trying to steal your password. And in order to understand

Omurchu - Direct/Levine

1 if that's what the code is doing, you have to have analyze
2 it and reverse engineer it and break it apart. And we used
3 tools to do that. And it can be quite complex and quite a
4 difficult process to understand exactly what the purpose is
16:02:15 5 of the code you're looking at.

6 **Q.** Okay.

7 And you used the term -- and I want to make sure we
8 understand the term -- malicious code. What is malicious
9 code?

16:02:23 10 **A.** Malicious code is bad code. It's code doing something
11 that the user would not like. So stealing passwords, for
12 example, is malicious, has malicious intent.

13 **Q.** Okay.

14 Now, in December 2008, did you receive a promotion?

16:02:41 15 **A.** I did.

16 **Q.** Tell me what was your promotion.

17 **A.** I was promoted to the manager of the team, first of
18 all, in Dublin and then in the U.S., manager of a team of
19 reverse engineers.

16:02:55 20 **Q.** Okay.

21 And when did you become the Director of the Security
22 Response Team?

23 **A.** I -- it was around that time, 2008, 2009. I can't
24 remember the exact date.

16:03:11 25 **Q.** Okay.

Omurchu - Direct/Levine

1 As the director of the Security Response Team, how
2 many direct reports do you have?

3 **A.** About ten.

4 **Q.** Okay.

16:03:19 5 And in the course of your work at Symantec, roughly
6 how many different pieces of malware or malicious code, to
7 use your term, would you say you've analyzed?

8 **A.** A thousand.

9 **Q.** Thousands?

16:03:33 10 **A.** Um-hum.

11 **Q.** Okay.

12 And just so we're on the same page, is malware and
13 malicious code the same thing or is there a difference?

14 **A.** It's the same thing, yeah. Malware is a software. So
16:03:49 15 that the normal word for a program is software, and so they
16 just took malicious in front of that and shortened it to
17 make it malware, but it's the same thing; malicious malware,
18 malicious code.

19 **Q.** If I say malicious code or software or malware, you'll
16:04:08 20 understand those all to mean the same thing?

21 **A.** Yes.

22 **Q.** Okay.

23 So I'd like to talk about your investigation into the
24 Bayrob Group and the Bayrob trojan. So first, why was
16:04:19 25 Symantec investigating the Bayrob Group and the Bayrob

Omurchu - Direct/Levine

1 trojan?

2 **A.** Well, it -- to begin with, we analyzed it just because
3 a customer had been infected with it and had lost some money
4 and they submitted it to us. And what had happened and if
16:04:36 5 the software was responsible for them losing their money, so
6 this is normal -- normal procedure of how we operate.
7 Customers will submit suspicious files to us as suspicious
8 code, and we determine for them if it -- what -- why it
9 exists, is it good, is it bad. And if it's bad, we protect
16:04:59 10 against it.

11 **Q.** So do customers submit malware to you manually or does
12 it automatically send up, uploaded from your antivirus
13 product?

14 **A.** Originally it was sent to us manually on disks.
16:05:16 15 People put it on disks and send it to us, but it's a little
16 bit outdated now. So normally people send it via website,
17 via e-mail, or it can be automatically uploaded from their
18 computer to our -- to our company.

19 **Q.** And when you receive malware or the sample of code
16:05:34 20 from a customer, what are you trying to do with it?

21 **A.** We're trying to protect against it. That's our
22 primary objective to protect against that piece of code or
23 any piece of code that looks similar to it.

24 **Q.** Okay.

16:05:48 25 And when did you personally start investigating the

Omurchu - Direct/Levine

1 Bayrob Group and the Bayrob trojan?

2 **A.** In 2007.

3 **Q.** And how long did your investigation continue?

4 **A.** Until 2016.

16:06:00 5 **Q.** All right.

6 **A.** September of 2016.

7 **Q.** What was it that ended your investigation?

8 **A.** The arrest of the -- of people behind it.

9 **Q.** Okay. See you were investigating the Bayrob Group for
16:06:14 10 roughly nine years?

11 **A.** Yes.

12 **Q.** And during that nine years, were you generally the
13 primary Bayrob investigator for Symantec?

14 **A.** I was the primary investigator, but we do have a large
16:06:27 15 team of people who analyze all sorts of code. So we
16 probably had ten or fifteen or more, I don't know, engineers
17 who analyzed the code over that period of time, but I was
18 the main engineer responsible for analyzing it.

19 **Q.** Were those ten or fifteen people working for you?

16:06:46 20 **A.** Some of them were, yes. We have -- we have a 24/7
21 support organization. So we have engineers who work all
22 over the world. But, certainly some of the people who
23 worked for me would have been analyzing that code.

24 **Q.** And you indicated that typically or sometimes Symantec
16:07:07 25 becomes aware of malware because they're submitted by a

Omurchu - Direct/Levine

1 customer.

2 Is that how the Bayrob trojan came to the attention of
3 Symantec?

4 **A.** Yes, that's right.

16:07:16 5 **Q.** Okay.

6 And I use the word trojan there, what is a trojan?

7 **A.** A trojan is just like malware, malicious code. A
8 trojan is like the famous story from ancient Greek of the
9 horse delivered to Troy. So the trojan horse, and inside it
16:07:37 10 was hiding the army, and the horse was brought inside the
11 gates of the defense and during the night, the army was able
12 to escape and attack from inside the castle.

13 So it's used -- in general terms, it's used to
14 describe something that presents itself as one thing but
16:07:54 15 actually does something else.

16 And we use it in the antivirus industry and securities
17 industry to mean a piece of software that presents itself as
18 one thing but actually does something else surreptitiously
19 hidden from the user. So, for example, present itself as a
16:08:13 20 gallery of pictures and the user would think they were
21 seeing pictures but the trojan part of it is that underneath
22 that, without the user knowing it, the code is actually
23 doing something malicious.

24 **Q.** Got it. So a trojan is a type of malware?

16:08:28 25 **A.** Yes.

Omurchu - Direct/Levine

1 Q. Okay.

2 And I want to talk about the main ways, I just want to
3 understand one of the main ways Symantec was investigating
4 the Bayrob Group.

16:08:40 5 So was one of the ways Symantec investigating the
6 Bayrob Group by analyzing the Bayrob Malware?

7 A. Yes.

8 Q. And how were you able to get copies of the Bayrob
9 Malware to analyze?

16:08:52 10 A. By getting them submitted from customers primarily.
11 That was the first way. So that was one way, looking at
12 spam e-mail to see if anything looked like Bayrob was
13 another way, installing the software on to our own
14 computers, and then waiting for our computers to get an
16:09:17 15 update, it was another way.

16 We have lots of different ways to source the files.

17 Q. Okay. And you used all of those ways?

18 A. Yes, as many as we can, any that we can to find
19 samples.

16:09:32 20 Q. Okay.

21 So now, once you got a copy of Bayrob Malware, was it
22 in a form that you could easily just read and analyze?

23 A. No, it's difficult to analyze it and to study it and
24 to understand what it does.

16:09:51 25 Q. What do you have to do in order to read the Bayrob

Omurchu - Direct/Levine

1 Malware in a form that you can read it and understand it?

2 **A.** We have to use tools. We have to use specialized
3 tools to be able to break the code apart and then look at
4 how it's organized and look at the capabilities of it, and
16:10:14 5 we run it on computers, on test computers and we observe the
6 activities, see what it is it's doing, where is it
7 connecting, you know, what files is it creating on the
8 computer.

9 We use debuggers and the tools, the actual names for
16:10:30 10 the tools we use are debuggers and disassemblers and hex
11 editors, and those are all specialized tools that allow you
12 to look inside a file and understand what that file is
13 actually trying to do.

14 **Q.** Let's go through each of those. I think the first one
16:10:44 15 you said was debuggers?

16 **A.** A debugger, yes.

17 **Q.** What's a debugger?

18 **A.** So a debugger is a tool that allows you to run code
19 and look at it as it's running. So you run Word on your
16:11:02 20 computer, and you want to understand what the code is doing.
21 So if you run it with a debugger, you can stop it at any
22 point, and you can say, you know, what it's just done, just
23 created a file, and/or if you wanted to see how someone just
24 clicked the button, you will use the debugger and say they
16:11:23 25 just clicked the button and the next thing that's about to

Omurchu - Direct/Levine

1 run is whatever that button was going to do. Say it's the
2 save button, you can then see when the person clicks the
3 save button. You can see the code that runs when you do
4 that.

16:11:36 5 So it allows you to see the instructions as the person
6 is using the program.

7 **Q.** Okay.

8 So a debugger. And you mentioned something called a
9 disassembler?

16:11:47 10 **A.** Yeah, a --

11 **Q.** What's a disassembler?

12 **A.** A disassembler -- so to assemble something is to put
13 it together. Disassemble is to take it apart. And the
14 program called a disassembler will take the software apart and
16:12:05 15 let you look at the individual instructions that are in
16 there. Again, using Word as an example, you know, there has
17 to be some code inside of the Word program that will save a
18 file to disk. And if you use a disassembler, you can open
19 up the Word program and you can see those instructions, and
16:12:23 20 you can isolate the instructions that actually write a file
21 to disk.

22 **Q.** Okay. And did you mention a third tool?

23 **A.** Hex editor is the third.

24 **Q.** What is a hex editor?

16:12:33 25 **A.** So a hex editor is another way to look inside a

Omurchu - Direct/Levine

1 program, and so --

2 **Q.** Let me start with what is hex?

3 **A.** Yeah, okay.

4 So ultimately, you know, inside the computer,
16:12:51 5 ultimately everything is 1's and 0's. That's how a computer
6 works. But for a human to read 1's and 0's is very
7 difficult. So to what they do is they have a program that
8 will convert the 1's to 0's into a different number format,
9 which is called hexadecimal, which has 16 numbers instead of
16:13:11 10 ten number numbers like a decimal has. And that's just
11 easier to understand how the program is written, I guess
12 for -- for a technical person for an engineer.

13 So when you open up a program with a hex editor,
14 generally what you see is you see -- on one side you see the
16:13:32 15 code, and then on the other side, you see the interpretation
16 of that code, so meaning associated with that code, and it
17 just makes it easier to open up a program and to understand
18 the basics of what's going on inside.

19 **Q.** So the program, the hex editor is translating what's
16:13:49 20 essentially 1's and 0's into something you can read?

21 **A.** Yeah, exactly.

22 **Q.** Okay.

23 So these are three types of programs that you're able
24 to use to be able to read and analyze the Bayrob Malware?

16:14:03 25 **A.** That's correct.

Omurchu - Direct/Levine

1 Q. Okay.

2 So you analyze the Bayrob Malware from customers. Did
3 you say that another way that Symantec investigated the
4 Bayrob Group was by infecting its own computers with the
16:14:21 5 Bayrob Malware?

6 A. Yes. A common way for us to look for updates from
7 malware is to install the malware on our own computer and
8 then wait to see if it gets updated.

9 Q. So how many computers did Symantec infect with the
16:14:38 10 Bayrob Malware?

11 A. About five computers altogether.

12 Q. Okay.

13 And where were the Symantec infected computers
14 located?

16:14:46 15 A. So primarily, they're located in our lab, which is in
16 Los Angeles, but we also had a computer in, I believe it was
17 in New York and one in Romania.

18 Q. Okay.

19 And how did infecting your own computers with the
16:15:06 20 Bayrob Malware help you to investigate the Bayrob Group?

21 A. Well, we could see what instructions were being sent
22 to the malware. So the malware was able to receive
23 instructions to do different activities, so we could monitor
24 those instructions as they were received. We could tell
16:15:24 25 what the malware was doing. And also we could find updates.

Omurchu - Direct/Levine

1 When the updates came down, we could analyze those updates,
2 compare them to the previous version and see what new
3 functionality had been added, as we understand what the
4 authors were -- what new features the authors were trying to
16:15:43 5 add and primarily allowed us to create protection to block
6 the Bayrob virus from getting on to our customers'
7 computers.

8 **Q.** Were the Bayrob Group also using the infected
9 computers as proxies?

16:16:00 10 **A.** Yes, they were.

11 **Q.** Okay.

12 And I want to bring up Exhibit 2037, which is a
13 demonstrative that the jury has previously seen, and I don't
14 know if you have seen this demonstrative before. But, would
16:16:19 15 this demonstrative help you explain how your computers were
16 being used as a proxy?

17 **A.** I don't see anything here on my screen.

18 MR. LEVINE: Oh, I'm sorry.

19 THE WITNESS: Okay.

16:16:30 20 MR. LEVINE: Can you let me know whether you
21 do see it?

22 THE WITNESS: Sure. Yeah, I see it now.

23 **Q.** Okay. So take a moment to look at that.

24 **A.** Uh-huh.

16:16:39 25 **Q.** Would that help you explain how your computers were

Omurchu - Direct/Levine

1 being used, your infected computers were being used as
2 proxies?

3 **A.** Yes, by -- you know, in this -- in this picture, the
4 laptop here is the infected computer. Is that what
16:16:56 5 you're --

6 **Q.** Well, if it would help you explain, let's assume the
7 laptop is the infected computer.

8 **A.** Yes.

9 **Q.** How is that -- how is your infected computer being
16:17:09 10 used as a proxy?

11 **A.** So a proxy allows -- if you have a proxy on your
12 computer, it allows traffic to flow through your computer
13 from one person into your computer, and out near the side.
14 And the benefit of a proxy is that it hides the original
16:17:28 15 source of the traffic. So somebody could connect it to my
16 computer and then they would have one address, they would
17 have one IP address, but when they connect out from my
18 computer to, for example, Gmail here, they don't -- they no
19 longer show their address. They show my address. So if
16:17:49 20 someone at Gmail is investigating this traffic, they think
21 the traffic is coming from my computer and they don't
22 realize that the traffic is actually coming from somewhere
23 else.

24 **Q.** Okay.

16:17:58 25 So we heard testimony earlier that the Bayrob was

Omurchu - Direct/Levine

1 proxying through infected computers. Were your -- some of
2 your computers some of the infected computers they were
3 proxying through?

4 **A.** Yes, that's correct.

16:18:11 5 **Q.** Okay.

6 Now of your five infected computers, you said there
7 was some in the US, and there was at least one in Romania.
8 Did one of them turn out to be more useful than the others?

9 **A.** Yes, the machine in the Romania turned out to be more
16:18:34 10 useful.

11 **Q.** And why was that?

12 **A.** It was because of the way the -- it's because the
13 authors were in Romania, and they like to connect to Romania
14 machines first before they connected to machines in the US.

16:18:51 15 And that was likely to try to protect their -- their
16 location.

17 So the first thing they would do is they would connect
18 from the machine to a proxy in Romania, and then they would
19 connect to another proxy in the US, and then they would
16:19:09 20 connect out, in this case, through the Gmail. And what that
21 means is that it becomes more and more difficult to track
22 their original location because they redirected through
23 multiple different proxies.

24 **Q.** So basically, your Romanian -- you had an infected
16:19:28 25 computer in Romania?

Omurchu - Direct/Levine

1 **A.** Yeah.

2 **Q.** And that computer was closer to the source?

3 **A.** Yes, yes, exactly. It was closer to the source, and
4 it was a preferred -- preferred to pick a computer that was
16:19:42 5 closer to the source as the first computer to connect to.

6 **Q.** Preferred by who?

7 **A.** By the Bayrob Group.

8 **Q.** Okay.

9 So were you more likely to be able to monitor Bayrob
16:19:58 10 activity on that computer in Romanian than in your infected
11 computers in the United States?

12 **A.** Yes.

13 **Q.** Okay.

14 Now, to clarify, if the Bayrob Group had infected my
16:20:09 15 computer and was using it for proxying through my computer,
16 would I be able to see what they were doing or were you
17 doing something special to monitor what they were doing?

18 **A.** Yeah, we were doing something special to monitor it.

19 **Q.** Okay.

16:20:24 20 What were you doing to monitor what the Bayrob Group
21 was doing on your infected computers?

22 **A.** So we were listening to the traffic. We have a
23 program; not just us. It's a program available that allows
24 you to listen and record the traffic that is coming into and
16:20:43 25 out of your computer.

Omurchu - Direct/Levine

1 So you can use that for just listening to the traffic
2 when you connect to Gmail, for example if you wanted to see
3 what was happening there. And it's used to diagnose network
4 problems and other things.

16:20:59 5 What we were doing was we were recording all the
6 information that was coming into our computer and passing
7 out the other side. And then we could use that collected
8 information to understand what was happening in that network
9 in that network traffic.

16:21:13 10 **Q.** Okay.

11 Now I just want make sure I understand you because
12 you're using the word traffic a lot. And when I think of
13 traffic, I think of what I'm going to face when I go home.

14 So what do you mean when you say traffic?

16:21:26 15 **A.** The instructions that are passing through the
16 computer. So when you -- I don't know. You want to check
17 the bus time table on a website, you know, you go to that
18 website and some pages come from that website down to your
19 computer, and that's how you're able to see the website.

16:21:45 20 And what we do is record all of that website, all of
21 the code on that website as it comes down to your computer.
22 We record all that information, and we can reconstruct your,
23 the website that you saw from that information.

24 **Q.** So would traffic include anything from the Internet
16:22:06 25 coming into the computer?

Omurchu - Direct/Levine

1 **A.** Yes.

2 **Q.** And would it also include anything from the computer
3 that's going out and onto the Internet?

4 **A.** Exactly.

16:22:14 5 **Q.** You said you have special tool, it's not just yours,
6 but can you say what the tool is called?

7 **A.** Sure. It's called Wire Shark.

8 **Q.** Is that software or hardware?

9 **A.** That's software.

16:22:22 10 **Q.** Okay.

11 It's a program called Wire Shark. What does Wire
12 Shark do?

13 **A.** Wire Shark listens to the traffic coming in and out of
14 the computer and records it into a file and then at a later
16:22:39 15 time, you can open that file and see exactly what happened,
16 what traffic came in and out during the time you were
17 recording it.

18 **Q.** Okay. You say -- I think you used the term "listens."

19 Now, I -- I have a tendency to personify things, but
16:23:00 20 is it listening to audio or is it -- what is it actually
21 doing?

22 **A.** No, it's not. It's listening to the -- we use the
23 term listen. It's recording the information coming over the
24 wire into your -- from the Internet into your computer.

16:23:16 25 **Q.** So it's recording data?

Omurchu - Direct/Levine

1 **A.** Yes, recording the data, yes.

2 **Q.** And in your experience, does Wire Shark produce
3 reliable and accurate electronic records of what the Bayrob
4 Group was doing over the infected computers?

16:23:29 5 **A.** Yes.

6 **Q.** Okay.

7 So you analyze malware you got from customers, and you
8 monitored your five infected computers. Were you also able
9 to access some information on the Bayrob Group's command and
16:23:47 10 control servers?

11 **A.** Yes, I was.

12 **Q.** Okay.

13 Now at a general level, what is a command and control
14 server?

16:23:56 15 **A.** Well, it's kind of in the name. It allows you to
16 control and send commands to, in this case, a virus that's
17 infected a computer.

18 So computer is infected, the virus is running on it,
19 and the virus needs to know what to do. And in order to
16:24:12 20 understand what it should do, or what happens is it connects
21 out onto the Internet to what we call a command control
22 server and asks for commands, and the attacker is able to
23 control the virus, via that command and control server.

24 **Q.** Okay.

16:24:28 25 I hate to do it to you. But, what is a server?

Omurchu - Direct/Levine

1 **A.** A server is just a powerful computer that's online.
2 It has better speed, it has better more memory, it has more
3 size. Generally it's available 24/7. It's not -- you know,
4 it's not on your counter at home where you turn it off at
16:24:53 5 night. It's on all the time under some sort of support.
6 Service is available if something happens to it.

7 **Q.** Okay.

8 So a command and control server then is a powerful
9 computer that's used to control infected computers?

16:25:10 10 **A.** Yes.

11 **Q.** All right.

12 Were you able to locate the Bayrob Group's command and
13 control servers?

14 **A.** Yes, I was.

16:25:19 15 **Q.** And when you would locate it -- first of all, how were
16 you able to locate it, the Bayrob Group's command and
17 control servers?

18 **A.** Just by running the malware, running the virus on our
19 computers and then recording where it's connected on the
16:25:42 20 Internet and by examining where it's connected, we could
21 determine where it's getting its commands from.

22 **Q.** And you said that you were able to access some
23 information that was actually on the Bayrob Group's command
24 and control servers; is that right?

16:25:58 25 **A.** That's correct.

Omurchu - Direct/Levine

1 Q. How were you able to do that?

2 A. By requesting the files from the -- from the server.

3 So making, like visiting a web page, visiting the command

4 and control server and picking up information from it. And

16:26:15 5 then the other way is looking to see if any of the traffic

6 on our infected computers was making requests through the

7 command and control center.

8 Q. So, first of all, you had to know the location of

9 where the command and control server was?

16:26:30 10 A. Uh-huh.

11 Q. Is that -- what kind of locations are we talking about

12 here? Are we talking data centers, are we talking homes, or

13 we talking -- what are we talking about?

14 A. Data centers, yeah, data centers, you know, think

16:26:44 15 companies that do this all the time that have, you know,

16 it's their job.

17 Q. Okay.

18 And servers were located within those data centers?

19 A. Yes.

16:26:57 20 Q. Where were those data centers located?

21 A. They were located in different places, but some of

22 them were in the U.S., one of them was in Dream Host was the

23 name of the company.

24 Q. Okay. What is Dream Host? Never heard of it.

16:27:13 25 A. Dream Host is a company that, you know, provides

Omurchu - Direct/Levine

1 servers to people. You can go and rent a server or buy a
2 server from them, and they will have it in their data center
3 and make it available to you 24/7 and support you, allow you
4 to do whatever it is that you want to do on your server and
16:27:33 5 for it to be available online at all times.

6 Q. Okay.

7 And I -- are most Dream Host customers legitimate,
8 like a legitimate thing for data hosting like this?

9 A. Yes, it's a huge company.

16:27:45 10 Q. Okay. All right.

11 So you analyzed malware from customers, you monitored
12 your infected computers, and you accessed some information
13 from the Bayrob Group's command and control server.

14 Did you also run your own undercover operation on
16:28:00 15 eBay?

16 A. Yes.

17 Q. All right.

18 We'll get to the details of that operation a lot
19 later, but at a general level, can you tell us what
16:28:10 20 undercover operation you did?

21 A. The Bayrob Group was trying to sell cars on eBay.

22 MR. O'SHEA: Objection.

23 THE COURT: Overruled.

24 THE WITNESS: And what I did was I pretended
16:28:28 25 to be a victim, and I signed up for an auction and created a

Omurchu - Direct/Levine

1 fake person so that I could participate and go ahead and
2 actually buy a car from that auction.

3 And I recorded all of that information so I could
4 understand how the Bayrob scheme in total worked.

16:28:48

5 **Q.** Okay.

16:29:02

6 So were the four main ways you investigated your
7 Bayrob Group analyzing malware from customers, monitoring
8 the infected computers, accessing information from the
9 Bayrob Group's command and control servers, and doing the
10 eBay undercover operation?

11 **A.** Yes.

12 **Q.** Okay.

16:29:12

13 So now I want to talk about what you learned from your
14 investigation. I want to start with how the Bayrob Group
15 would infect people with malware.

16 And I'd like to show you what has been -- well, you
17 know what? We're at 4:29, your Honor, and --

18 THE COURT: That's all right. I made other
19 arrangements.

16:29:30

20 MR. LEVINE: Okay.

21 THE COURT: So you don't have to be concerned
22 about my issue.

23 MR. LEVINE: We are now in the portion where
24 I'm going to start showing exhibits and --

16:29:36

25 THE COURT: Let's see what happens.

Omurchu - Direct/Levine

1 MR. LEVINE: Okay.

2 Q. So I'd like to show the witness what has been
3 previously marked as Government's Exhibit 1421, which is a
4 nine-page exhibit. And I'd like to just show it to the
16:29:51 5 witness right now.

6 Mr. Omurchu, could you let me know whether you see it?

7 A. Yes, I see it now.

8 Q. Okay. Great.

9 Can you tell me what is Government's Exhibit 1421?

16:30:06 10 A. These are pictures of e-mails that were sent by the
11 Bayrob Group.

12 Q. What kind of e-mails on a general level?

13 A. They're spam e-mails with viruses attached.

14 Q. Okay.

16:30:23 15 And what is the source? How do you get the
16 screenshots that are in Government's Exhibit 1421?

17 A. My infected machines were instructed to send spam, and
18 this is the spam that they were instructed to send.

19 Q. So the malware instructed your machine to send these
16:30:42 20 e-mails?

21 A. That's correct.

22 Q. Okay.

23 And does Government's Exhibit 1421 contain a fair and
24 accurate screenshot of the spam that you saw through your
16:30:51 25 infected computers?

Omurchu - Direct/Levine

1 **A.** Yes, it does.

2 **Q.** Okay.

3 I'd like to move to admit Government's Exhibit 1421.

4 MR. O'SHEA: Let me double check, but I don't
16:31:02 5 think we have an objection. It's 12 pages long, your Honor.
6 Just a few seconds.

7 THE COURT: No problem.

8 MR. LEVINE: And just to clarify, I believe
9 there's a translation -- some of the pages are translated
16:31:13 10 and the translation is at the end. So that's why the
11 discrepancy in page numbers.

12 MR. O'SHEA: No objection to that exhibit,
13 1421, your Honor.

14 THE COURT: Mr. Goldberg?

16:31:48 15 MR. GOLDBERG: No objection, your Honor.

16 BY MR. LEVINE:

17 **Q.** All right.

18 So let's look at -- if we could publish to the jury
19 the first page of 1421.

16:31:57 20 Can you tell us what we're seeing here on the first
21 page?

22 **A.** This is -- this is an e-mail trying to trick users
23 into executing virus, running the virus on their machine.
24 And it's saying that the Facebook account has been
16:32:22 25 restricted, and in order for them -- in order for them to

Omurchu - Direct/Levine

1 get back on for Facebook, they need to open the file and run
2 it.

3 Q. Okay. And what does the file contain?

4 A. The file contains the Bayrob Malware.

16:32:39 5 Q. Okay.

6 So this is a malicious e-mail your computer was
7 instructed to send?

8 A. That's correct.

9 Q. All right. Can you look at the second page of this
16:32:50 10 exhibit? And what is this one?

11 A. So the way my computer was instructed to send e-mail
12 was that I would receive -- so this is -- I would receive a
13 template that was -- that I was asked -- that my computer
14 was asked to send out to other computers. And these are the
16:33:17 15 types of templates that I would receive, "Did you check out
16 the pictures that I sent you?" And then it would be a link
17 associated with that. And that link would point to a copy
18 of a Bayrob Malware. And if you ran the file at that link,
19 it would infect your computer.

16:33:36 20 Q. So the e-mail said, "Did you check out the pictures I
21 sent you," and then what is that below the question?

22 A. That's a link to the virus.

23 Q. And it looks like it says Dropbox. What is Dropbox?

24 A. That's a -- Dropbox is a website where you can store
16:33:55 25 files instead of having to embed them in the e-mail.

Omurchu - Direct/Levine

1 Instead, you could send a link instead.

2 Q. So does that mean that the Bayrob Group had their
3 malicious software, the trojan on Dropbox?

4 A. Yes.

16:34:09 5 Q. And so what would happen if the user received this
6 e-mail and clicked on that link?

7 A. They would get infected.

8 Q. Okay.

9 And you said -- by the way, you said your computer was
16:34:24 10 asked to send these?

11 A. Yeah.

12 Q. Was your computer asked or told to send these?

13 A. My -- to use the command and control term that we used
14 earlier, my machine was commanded to send these e-mails.

16:34:39 15 Q. Okay.

16 Let's look at the third page here. Take a moment to
17 look at that. And if you can tell us, what is this one?

18 A. This is a similar situation but in Romania. It's an
19 e-mail with a copy of the Bayrob Malware attached. And if
16:35:04 20 you run the file, zip file, if you run the file that's in
21 there, you'll get infected.

22 Q. And to be clear, would you have to do anything on your
23 computer to make these malicious e-mails send out or was
24 that happening automatically?

16:35:18 25 A. No. That was happening automatically and in the

Omurchu - Direct/Levine

1 background, you know. If a regular person's computer was
2 infected, they wouldn't see any of this. This was all
3 hidden. But because there was more activity on my computer,
4 I could see these instructions.

16:35:32 5 **Q.** Let's see -- can we see the next page, please? What
6 is this showing?

7 **A.** So this is showing a collection of e-mails that my
8 computer was commanded to send. And you can see that the
9 "from" address is similar but the two addresses are
16:35:55 10 changing. So this is the spam that is being sent out and on
11 the right-hand side in the gray panel. You can see the
12 content of the e-mail. And down at the bottom, on the
13 right-hand side, it says go through the attached file, view
14 all of the information. When asked, enter the keyword, and
16:36:16 15 it gives you the password that you need in order to run the
16 attachment.

17 And the subject here, which is further up, it says,
18 "To Artsy Babe," the person who is receiving it, "Artsy
19 Babe, your medical analysis reveals HIV-2 infections."

16:36:36 20 **Q.** AIDS?

21 **A.** AIDS. That's correct, yes.

22 **Q.** So this e-mail purports to be the result of -- this
23 e-mail purports to be to test results showing you have AIDS?

24 **A.** Yes, that's correct.

16:36:51 25 **Q.** And what would happen if you clicked on the

Omurchu - Direct/Levine

1 attachment?

2 **A.** You would get infected with the Bayrob Malware.

3 **Q.** Could we -- let's look at the next page. What is this
4 page?

16:37:10 5 **A.** This is the text of the -- of the e-mails they were
6 sending out that we were talking about being infected with
7 HIV-2. This was the content of that e-mail that was shown
8 on the last slide and shows more clearly here and pretending
9 to be from a doctor, and it's saying you must contact me as
16:37:38 10 soon as possible, regarding -- you know, because you're
11 infected and it was instructing you what to do, how to open
12 the file that was attached because the father was attached,
13 the keyword associated with it, you need to use to open
14 that, and then once you open that and you ran the file
16:37:55 15 inside, you would get infected with the Bayrob Malware.

16 **Q.** And what is all that BR stuff I see in there?

17 **A.** That's -- it's an HTML, a language used for making web
18 pages and this was to help format the e-mail correctly, so
19 that when you would see it in Gmail or hotmail, wherever
16:38:18 20 reading it, it would be formatted more correctly so the
21 angle brackets and the B means to make what's inside that
22 area bold. And the angle brackets be/or is the break, which
23 means create a new line here. So it's just formatting
24 information.

16:38:34 25 **Q.** So it would -- you wouldn't -- if I receive this AIDS

Omurchu - Direct/Levine

1 e-mail, I wouldn't see that BR stuff like that?

2 **A.** No, you would not see that when you read the e-mail.

3 **Q.** And it would be formatted in a way that looks
4 legitimate?

16:38:46 5 **A.** Yes.

6 **Q.** Could we look at the next page of this exhibit? What
7 are we looking at here?

8 **A.** So this is more spam being sent. This spam was to --
9 advertising iPads and tablets for sale, and this e-mail is
16:39:04 10 made to look like it comes from Wal-Mart but doesn't
11 actually come from Wal-Mart but made to look like it comes
12 from Wal-Mart. And the content of the e-mail looks similar
13 to the Wal-Mart -- the layout and the graphics look similar
14 to the Wal-Mart store, but this is not from Wal-Mart. This
16:39:23 15 is e-mail, spam that my computer was coming out to sent.

16 **Q.** And could this spam give you the virus as well?

17 **A.** No, this spam didn't give you the virus. This spam
18 tried to sell you iPads and tablets that will never arrive.

19 **Q.** Okay.

16:39:41 20 So what would happen if I clicked on one of the links
21 here?

22 **A.** So if you click one of the links, you would be taken
23 to a site that would ask for your credit card and your
24 credit card number would be stolen at that point.

16:39:53 25 **Q.** Okay.

Omurchu - Direct/Levine

1 Let's look at the next page. Is this just showing the
2 bottom of the scrolling down in the same e-mail.

3 **A.** Yes, that's correct.

4 **Q.** All right. Let's look at the next page. Can you
16:40:07 5 describe this?

6 **A.** So this is more e-mail that my infected computer was
7 instructed to send. This is pretending to be Norton
8 AntiVirus, the company I work for. So it has Symantec down
9 at the bottom. I work for Symantec. And it's pretending to
16:40:25 10 give you one-year free trial for Norton Security, which is
11 ironic because it's not protecting you. It's actually
12 infecting you with a virus instead.

13 **Q.** Okay. So Norton Security, that's your product?

14 **A.** Yes, that's our product.

16:40:42 15 **Q.** Also called Norton AntiVirus?

16 **A.** Yes.

17 **Q.** This is not giving you Norton AntiVirus?

18 **A.** No, it's not giving you Norton AntiVirus. It's
19 pretending it's giving you Norton AntiVirus but you open the
16:40:55 20 file attached here, you run the file that's in there, you
21 would get infected with the Bayrob Malware.

22 **Q.** So is this a good example of what you were talking
23 about as a trojan; looks like it's giving you something good
24 but giving you something bad?

16:41:09 25 **A.** Yes, exactly, yes.

Omurchu - Direct/Levine

1 Q. Okay.

2 Can we look at the next image? What is this one here?

3 A. This is more spam that my computer was commanded to
4 send, to send, and it is pretending to be from Western
16:41:26 5 Union. And it is saying that you have \$645. It's available
6 for you to pick up at Western Union. And to receive the
7 money, you need to print out the document that is attached,
8 and the idea is that you will open the attached document and
9 that you'll get infected.

16:41:43 10 Q. Okay.

11 So this is purporting to be from Western Union?

12 A. That's correct, yes.

13 Q. I've seen other versions of this where you actually
14 see the Western Union logo on top. Is there a reason we
16:41:53 15 don't see it here in this one? You also don't see the image
16 at the bottom.

17 A. Yes, you know the image may not have been available
18 when I took this screenshot.

19 Generally, the images that are shown inside the e-mail
16:42:12 20 are actually taken directly from the Western Union website
21 so they look -- they are the real picture. And so I don't
22 know what that picture is meant to be but generally, they
23 would have the Western Union logo embedded there to make it
24 look more real.

16:42:28 25 Q. Okay.

Omurchu - Direct/Levine

1 And this is another attachment. If you click on it,
2 you get the malware?

3 **A.** Yes.

4 **Q.** Let's go to Page 10.

16:42:37 5 So we're now going to get into the FBI translation of
6 the two that were in the main. So if you could go to the
7 next page.

8 So this was the Dropbox that we looked at earlier,
9 correct?

16:42:52 10 **A.** Yes.

11 **Q.** And if we could go to the next page, final page.
12 That's -- all right. Yes. And can you tell us -- this is
13 translated from Romanian. Can you tell us what this e-mail
14 is?

16:43:14 15 **A.** Yes.

16 So this is another scheme to try and get someone to
17 execute the file that's attached to the e-mail. This says,
18 "Marion, you're a winner we can party with family. To view
19 the attached document only to date, redeem the offer select
16:43:31 20 the desired location now or collect the promotion today in
21 euros. Download attached file, view it and complete it.
22 Note, document is valid exclusively on the Microsoft windows
23 platform. Have a successful party."

24 And this is pretending to be from a hotel, Hotel
16:43:50 25 Roberto Sinaia Company. And again, this is false pretense.

Omurchu - Direct/Levine

1 They're pretending that you've won, that you're a winner,
2 that you've won a weekend party but you haven't. And if you
3 open the attachment, you get infected with the Bayrob
4 Malware instead.

16:44:07 5 So all of these are schemes to entice the receiver to
6 open the attachment and run it.

7 **Q.** So who did the Bayrob Group send, who would they send
8 this type of spam to?

9 **A.** They would send it to anyone that they could, any
16:44:24 10 e-mail address they could find. They had lots of different
11 ways to collect e-mail addresses and part of their operation
12 was focused on collecting people's e-mail addresses so they
13 could then send e-mails like this.

14 THE COURT: Mr. Levine, it's a good place to
16:44:41 15 stop?

16 MR. LEVINE: Sure, your Honor.

17 THE COURT: Ladies and gentlemen, we will
18 adjourn for the evening. Please remember the admonition.
19 Do not form any opinion regarding this matter. Do not talk
16:44:51 20 about the case amongst yourselves or with anyone else.

21 Please be downstairs at 9:00 A.M. We will call for
22 you and bring you up as a group. So 9:00 A.M. Have a good
23 evening, everyone.

24 All rise for the jury.

16:45:39 25 (Proceedings in the absence of the jury:)

1 THE COURT: Folks, if you could have a seat,
2 please.

3 MR. O'SHEA: One thing, Judge, and to state
4 the obvious, this witness is on the stand. I assume no one
16:45:47 5 converses with him during the night about his testimony.
6 He's under oath and --

7 THE COURT: Sir, one moment, please.

8 MR. LEVINE: Of course, your Honor. There's
9 not -- no communications with witnesses while they're on the
16:46:01 10 stand.

11 MR. O'SHEA: Very good. That's it, Judge.

12 MR. BROWN: We do have a witness that's a
13 coordinator.

14 THE COURT: Right.

16:46:07 15 MR. O'SHEA: Sometimes it happens by accident.
16 That's all, you know.

17 THE COURT: Right. I just want the witness to
18 know that the lawyers for the Government will not be
19 conversing with you tonight.

16:46:18 20 THE WITNESS: Okay.

21 THE COURT: Or tomorrow morning. All right.

22 We have agreed that every night, we will go over the
23 exhibits that have been discussed. So I have the list from
24 yesterday and today and see if you are in a position to even
16:46:38 25 offer them and if you're in a position to object or not

1 object.

2 Please be seated, folks. Please.

3 Government's Exhibit 1480 to 1679, are you in a
4 position at this point in time to offer them?

16:46:57 5 MR. LEVINE: No. We're not offering them,
6 your Honor.

7 THE COURT: I'm sorry?

8 MR. LEVINE: No, your Honor.

9 THE COURT: I didn't hear the end of that.

16:47:03 10 MR. LEVINE: No, your Honor.

11 THE COURT: Oh, I'm sorry. I thought you said
12 not at this time. Are you not offering them at all?

13 MR. LEVINE: I don't anticipate that we're
14 going to offer that range of exhibits.

16:47:16 15 THE COURT: I apologize -- I'm sorry,
16 Mr. Levine. I guess I didn't hear. I do apologize to you.
17 Okay.

18 So as of right now, you are not offering them and you
19 don't anticipate offering them unless circumstances change?

16:47:30 20 MR. LEVINE: Correct, your Honor.

21 MR. O'SHEA: And what was the range of those
22 exhibits?

23 THE COURT: 1480 to 1679.

24 MR. GOLDBERG: Those are the complaints.

16:47:41 25 MR. O'SHEA: All right.

1 THE COURT: Mr. Levine, the next one, 1320.

2 MR. LEVINE: Yes, 1320, your Honor, is the CD
3 of Read Notify e-mails.

4 THE COURT: Right.

16:48:00 5 MR. LEVINE: We would offer that into
6 evidence.

7 THE COURT: And you are prepared at this time?

8 MR. LEVINE: Yes, but I --

9 THE COURT: Any objection, Mr. Goldberg?

16:48:09 10 MR. GOLDBERG: I believe so, your Honor.

11 MR. O'SHEA: Yes. Oh, sorry. Go ahead.

12 MR. GOLDBERG: This is, I think, the disk
13 containing 19,000 e-mails. And I think we discussed the
14 words and the statements of, quote, coconspirator that are
16:48:34 15 contained in the e-mails would be admissible as an
16 exception, and I think that the Government respected that
17 ruling going through the examination of the witness.

18 It's the words and statements coming back that we
19 maintain are hearsay.

16:48:49 20 THE COURT: Okay.

21 MR. GOLDBERG: And there's 19,000 of them.

22 THE COURT: Okay. Before I call on you.

23 MR. O'SHEA: Yes, ma'am.

24 MR. LEVINE: We're not planning to let the
16:48:57 25 jury load the CD and read any of the 19,000 e-mails. The

1 e-mails that we're going to present to the jury will be
2 individually presented to the jury. What the CD simply
3 represents is what witnesses Chris Drake and Special Agent
4 Diaz says is an accurate compilation of the 19,000
16:49:19 5 e-mails --

6 THE COURT: But I can't allow a CD of 19,000
7 e-mails. I can't admit them into evidence and then tell the
8 jurors but no, you're not allowed to look at them. So I
9 think you have to be very specific as to what in 1320 you
16:49:35 10 are offering into evidence. And if you're not prepared at
11 this point in time to do so, that's fine.

12 MR. O'SHEA: I think I understand what they're
13 doing, Judge. It kind of makes sense. Guys, just take a
14 picture of the CD, mark it as an exhibit. How's that? If
16:49:51 15 the point you're making is that we have a CD with this -- I
16 mean that's the way you handle that, I think.

17 THE COURT: We also have testimony.

18 MR. O'SHEA: Yeah, that exists.

19 MR. LEVINE: All right. So we will figure
16:50:03 20 that one.

21 THE COURT: Fair enough. Fair enough.

22 1324.

23 MR. LEVINE: Yes, we would like to offer that
24 e-mail, subject to redaction of the victim statements in
16:50:22 25 that.

1 THE COURT: Perhaps we need to wait until the
2 redaction is done. So we'll hold off on that one.

3 MR. LEVINE: Okay.

4 THE COURT: 1325.

16:50:32 5 MR. LEVINE: Same situation, your Honor.

6 THE COURT: Fair enough. So you're not going
7 to offer it yet?

8 MR. LEVINE: Correct.

9 THE COURT: 2036 and 2037 are demonstrative
16:50:41 10 may I assume you're not offering those?

11 MR. LEVINE: Correct, your Honor.

12 THE COURT: All right.

13 1893.

14 MR. LEVINE: Not at this time, your Honor,
16:51:09 15 we'll have to do some redaction.

16 THE COURT: Fair enough.

17 1322.

18 MR. LEVINE: Subject to redaction, your Honor.

19 THE COURT: 1869.

16:51:25 20 MR. LEVINE: We have to take a look at that
21 one, your Honor.

22 THE COURT: All right.

23 MR. LEVINE: Not at this time, your Honor.

24 MR. O'SHEA: 1869, no? Withdrawn for now?

16:52:02 25 THE COURT: Well, it's not offered. It's not

1 withdrawn, just not offered yet.

2 MR. McDONOUGH: Excuse me, your Honor.

3 There's a juror that needs to come in to get something.

4 THE COURT: Oh.

16:52:13 5 MR. McDONOUGH: She's waiting outside.

6 THE COURT: Did she hear?

7 MR. McDONOUGH: No.

8 THE COURT: 3882 has been admitted. 385 has
9 been admitted. 1896.

16:54:20 10 MR. LEVINE: That's a certified copy of the
11 records, and they were stipulated to.

12 MR. O'SHEA: The authentication was but I'm
13 pretty sure this is just the net, right? I think what
14 happened was that -- for instance, in the document itself,
16:54:39 15 Judge, it says what Danet purportedly does for a living. I
16 assume Mr. Danet will be on the stand. He's one of --

17 THE COURT: You're just not prepared right
18 now?

19 MR. O'SHEA: Not right now, and it's only --
16:54:53 20 to authentication, yes, to admissibility, no.

21 THE COURT: I understand. We'll address it
22 later. 1895 you're not offering that. I believe that's
23 demonstrative. Am I correct?

24 MR. LEVINE: Correct.

16:55:13 25 THE COURT: 1897 has been admitted. 2429 has

1 been admitted. I'm going too fast, tell me.

2 MR. O'SHEA: What was the last one you just
3 did, Judge?

4 THE COURT: 2429. And then prior to that,
16:55:36 5 1897. Have both been admitted.

6 The 2429 are the wax seals and then I said 1897 has
7 also been admitted.

8 MR. O'SHEA: That's just the photograph.

9 THE COURT: And then 402.

16:56:17 10 MR. LEVINE: Yes. We're not prepared to admit
11 that at this time.

12 MR. O'SHEA: 402, not at this time.

13 THE COURT: 4.

14 MR. LEVINE: 4. Oh, the Number 4.

16:56:38 15 Not at this time.

16 MR. O'SHEA: Okay.

17 THE COURT: 2008 has been admitted. And
18 again, if I state anything that's not accurate, I expect
19 that you'll --

16:56:56 20 MR. O'SHEA: Double checking, Judge. That's
21 all.

22 THE COURT: Tell me if I'm going too fast.

23 MR. O'SHEA: Oh, that's just the physical lap

24 --

16:57:01 25 THE COURT: That's -- that's the laptop.

1 MR. O'SHEA: Okay.

2 THE COURT: 399 has been admitted. That's the
3 phone. 2274 has been admitted.

4 MR. O'SHEA: 2274 is again what?

16:57:32 5 MR. BROWN: The hard drive.

6 MR. O'SHEA: Sure.

7 THE COURT: 1321.

8 MR. BROWN: 1421?

9 THE COURT: 1321.

16:57:46 10 MR. LEVINE: No, we're not going to offer that
11 into evidence at this time, your Honor.

12 THE COURT: And then, folks, 1328, 29, and 30.

13 MR. LEVINE: So those --

14 THE COURT: Have already been admitted.

16:58:09 15 MR. O'SHEA: Are those the ones we agreed to
16 redact anything relative to the victims' statements?

17 MR. LEVINE: Yes.

18 MR. O'SHEA: Okay. So admitted with
19 redactions.

16:58:28 20 THE COURT: And, folks, I just assume they
21 were because they were shown to the jury and nothing was
22 said to me.

23 MR. O'SHEA: The unredacted --

24 THE COURT: That's our understanding.

16:58:36 25 MR. O'SHEA: The unredacted portions were

1 shown to the jury, Judge. We agreed to do that. So we'll
2 get -- we'll figure that out.

3 THE COURT: All right. Fair enough. 1421 has
4 been admitted. Again, I'm assuming it was shown.

16:58:54 5 MR. LEVINE: Yes, your Honor.

6 MR. O'SHEA: What's that again?

7 MR. LEVINE: The spam.

8 MR. O'SHEA: All right. Just the ones we just
9 did. Yep.

16:59:04 10 THE COURT: All right.

11 I believe, unless I missed something, I believe that's
12 everything, all the exhibits that have been discussed
13 yesterday and today.

14 MR. O'SHEA: I believe so, Judge. Yes.

16:59:16 15 THE COURT: Mr. Levine, did I miss anything?

16 MR. LEVINE: I think that's right, your Honor.
17 I would have to confer.

18 MS. CHANDLER: 2037.

19 THE COURT: That's demonstrative.

16:59:26 20 MR. LEVINE: That was a demonstrative.

21 MS. CHANDLER: Okay.

22 MR. LEVINE: But we'll confer.

23 THE COURT: Keep me on my toes here. So
24 please -- tell me if you -- I want to make sure I did get
16:59:37 25 everything.

1 MS. CHANDLER: I believe so.

2 THE COURT: Mr. Goldberg, did I miss anything?

3 MR. GOLDBERG: I don't think so, Judge.

4 MR. O'SHEA: I'm good, Judge.

16:59:44 5 THE COURT: Okay. And again, folks, I know

6 this isn't going to be hard and fast, you know. Everyday

7 we'll try to see what we can address, understanding there

8 are times you're not going to be in a position yet to

9 actually offer them, and you folks may be -- not be in a

17:00:01 10 position to know whether you're objecting. But at least it

11 gets us a little more organized.

12 MR. O'SHEA: Sure.

13 THE COURT: All right. We're in adjournment.

14 MR. BROWN: Thank you, your Honor.

17:00:11 15 MR. LEVINE: Thank you, your Honor.

16 THE COURT: All right.

17 (Proceedings adjourned at 5:00 p.m.)

18

19

20

21

22

23

24

25

1	DIRECT EXAMINATION OF STACY DIAZ	82
2	CROSS-EXAMINATION OF STACY DIAZ	178
3	CROSS-EXAMINATION OF STACY DIAZ	190
4	REDIRECT EXAMINATION OF STACY DIAZ	197
5	DIRECT EXAMINATION OF YVONNE LIDDY	206
6	DIRECT EXAMINATION OF CHRISTOPHER DRAKE	234
7	CROSS-EXAMINATION OF CHRISTOPHER DRAKE	271
8	REDIRECT EXAMINATION OF CHRISTOPHER DRAKE	275
9	RECROSS-EXAMINATION OF CHRISTOPHER DRAKE	277
10	DIRECT EXAMINATION OF LIAM OMURCHU	284

11

12

C E R T I F I C A T E

13

14

15

16

17

18

19

20

21

22

23

24

25

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

s/Shirle Perkins
Shirle M. Perkins, RDR, CRR
U.S. District Court - Room 7-189
801 West Superior Avenue
Cleveland, Ohio 44113
(216) 357-7106